TRIALS CONTENTS PAGE

Interoperability Trials

Coalition Warrior Interoperability Demonstration trials for 2007 are listed in trial number order below, cross referenced to sites where they can be observed during the demonstration June 18 to 21.

OBJECTIVES KEY
1. CROSS-DOMAIN DATA SHARING ■
2. INTEGRATED INTELLIGENCE ■
3. INTEGRATED OPERATIONS ■
4. INTEGRATED LOGISTICS ■
5. INTEGRATED PLANNING ■
6. INTEGRATED COMMUNICATIONS ■

TRIAL NO.	SYSTEM TITLE (ACRONYM OR SHORT NAME)	USEUCOM	USNORTHCOM	DAHLGREN	SPAWAR	HANSCOM	CANADA	NEW ZEALAND	UNITED KINGDOM	NATO	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	OBJECTIVE/S ADDRESSED	PAGE NO.
IT01.01	Compartmented High Assurance Information Network (CHAIN)	■	■	■	■	■					USNORTHCOM	Raytheon	**1**,3,4,5	3
IT01.05	Trusted Gateway System (TGS) Guard			■	■			■			US Air Force	US Air Force	**1**	3
IT01.17	Cross Domain Collaborative Information Environment/Collaboration Gateway (CDCIE/CG)		■	■	■	■					US Air Force, USJFCOM, FBI	Trident Systems, Inc., leads more than 12 other companies	**1**,2,3,5	4
IT01.28	NET/X eToken Security System, Deployable Communicartions System (NET/X)		■	■	■						USJFCOM	FED-COMM USA, Inc.	**2**	4
IT01.43	Mobile Forces Solution - Subnet Relay (MOFS-SNR)				■					■	Germany	T-Systems Enterprise Services GmbH	**1**	5
IT01.54	Collaborate-Access-Browser (CAB)	■	■	■	■	■		■			NSA	Essex Corporation	**1**	5
IT01.55	Assured File Transfer (AFT)	■		■	■	■		■			NSA	CTC, Essex Corporation,Tresys Technology	**1**	6
IT01.56	Dual Diode (One-Way) Data Transfer System (Dual Diode)				■		■	■			Canada	Owl Computing Technologies, Inc.	**1**	6
IT01.61	INTEGRITY Secure Workstation (INTSecWS)						■				Canada	Green Hills Software, Inc.	**1**	7
IT01.63	Coalition Assured Sharing Environment (CASE)		■	■							DISA	General Dynamics	**2**	7
IT01.86	Federated Identity Mangement System (FIDMS)		■	■		■					USJFCOM	BearingPoint, Hewlett Packard	**1**	8
IT01.87	Federated Security (FS)			■							USJFCOM	SAIC, IBM, Sun	**2**	8
IT02.06	Italian Navy Maritime Command and Control Information System (MCCIS-Italy rel. 5.2)				■					■	Italy	MARITEL-Roma	**2**	9
IT02.16	Deployable Geospatial Database (DGDB)		■				■				Canada	Canada	**2**	9
IT02.21	Commercial Joint Mapping Tool Kit (CJMTK)		■	■	■				■		NGA	Northrop Grumman Corporation	**2**	10
IT02.37	Rapid Force Warning (RFW)				■					■	US Army	US Army	**2**	10
IT02.57	Automatic Ingest, Mosaic and Mapping System (AIMM)		■	■	■		■				Canada	PCI Geomatics.	**2**	11
IT02.88	AdLib			■				■			USNORTHCOM	EchoStorm, Inc.	**2**	11
IT03.09	Global Personnel Recovery System (GPRS)	■	■	■							USJFCOM	Innovative Solutions International	**2**,3,4,5	12
IT03.14	Coalition Secure Management and Operations System (COSMOS)	■		■		■			■	■	OSD, USEUCOM, DISA	DISA, NSA, CDM	**3**,6	12
IT03.22	Scalable Mesh Networks				■						US Navy	OrderOne Networks	**3**,2	13
IT03.27	Integrated Information Management System (IIMS)			■							US Army, US Air Force	US Army, US Air Force	**3**	13

OBJECTIVES KEY
1. CROSS-DOMAIN DATA SHARING ■
2. INTEGRATED INTELLIGENCE ■
3. INTEGRATED OPERATIONS ■
4. INTEGRATED LOGISTICS ■
5. INTEGRATED PLANNING ■
6. INTEGRATED COMMUNICATIONS ■

TRIAL NO.	SYSTEM TITLE (ACRONYM OR SHORT NAME)	USEUCOM	USNORTHCOM	DAHLGREN	SPAWAR	HANSCOM	CANADA	NEW ZEALAND	UNITED KINGDOM	NATO	GOVERNMENT SPONSOR	GOVERNMENT/ CORPORATE DEVELOPER/S	OBJECTIVE/S ADDRESSED	PAGE NO.
IT03.30	Spatio-Temporal Analysis for Rapid Tasking (START)					■					US Air Force	The MITRE Corporation	3	14
IT03.31	Coalition Infrared Data Processing (CIDP)	■		■					■		US Air Force	Space and Missile Center, Missile Defense Agency	3,5	14
IT03.38	Collaborative Decision Aid (CDA)		■	■			■				USNORTHCOM	ARINC Engineering Services, LLC	3,5	15
IT03.39	Command, Control, Communications, Computers and Intelligence Defense (C4I Defense)	■		■		■	■				Italy	SELEX-SI SpA	3	15
IT03.48	Air Support Operations Center with Close Air Support System (ASOC Gateway with CASS)			■							US Air Force	US Air Force, US Navy	3	16
IT03.58	US Coast Guard Information Sharing and Communications (USCG IS&C)		■	■							US Coast Guard	US Coast Guard	3	16
IT03.70	Coalition open Joint Operations Picture (CoJOP)	■	■	■	■	■	■	■	■		UK	Fujitsu Services	3,5	17
IT03.71	MobiKEY Identity Based Access Drive (Mo-biKEY IBAD) and Defense Identity Management Network (DEFIMNET)	■	■	■	■	■	■				Canada	Route1, Inc.	3,5	17
IT03.75	Mobile Tactical Edge Network (MTEN)		■	■							USNORTHCOM	Professional Software Engineering, Inc., pTerex, LLC	3	18
IT03.80	Riverbed Information Optimization System (RIOS)	■	■	■		■	■				US Air Force, DISA	C2I Solutions, Riverbed	3,4	18
IT04.79	Event-based Common Operational Picture (ECOP)		■	■	■	■					NGB	Booz Allen Hamilton	3,4,5	19
IT05.08	Joint Strike Fighter (JSF) Offboard Mission Support Environment (OMSE)			■		■			■		JSF Program Office	Lockheed Martin, Systematic Software Engineering, Naval Mission Planning	5,1	19
IT05.12	ID-MAP: Situational Awareness, Visualization and Collaboration (ID-MAP)		■	■	■						USNORTH-COM, US Coast Guard	General Dynamics	5,2,3	20
IT05.59	Mission Planning System (MPS)					■	■	■			US Air Force	Collaboration Technologies, Inc.	3,5	20
IT05.78	Next Generation - Joint Information Exchange Environment (NG-JIEE)		■	■	■	■					NGB	Koniag Services, Inc.	5	21
IT06.04	Tactical Emergency Asset Management (T.E.A.M.)		■		■						USNORTHCOM	Quantum Research International	6	21
IT06.13	Global Information Grid Quality of Service Edge Solution for Interoperability (GIG QoS ESI)			■	■		■				US Army	DSCI	6	22
IT06.15	Geolap		■				■		■		Canada	Canada	6	22
IT06.36	Joint Network Defense and Management System (JNDMS)						■				Canada	MacDonald Dettwiler and Associates (MDA)	6	23
IT06.42	HotZone 4010/4020 (HZ4010)				■						US Navy	Trimax Wireless, Inc.	3,6	23
IT06.53	Weapons of Mass Destruction Collaborative Advisory Response System (WMD CARS)	■	■			■	■				USNORTHCOM	Defense Threat Reduction Agency (DTRA)	3,5	24
IT06.66	Internet Protocol Interoperability and Collaboration System (IPICS)		■	■		■					Canada	Cisco Systems, Inc.	6	24
IT06.74	Security Information Management for Enclave Networks (SIMEN)		■	■		■	■				US Air Force	The MITRE Corporation	1,6	25
IT06.89	Enhanced Video Text and Audio Processing (eVITAP)		■	■	■		■	■			US Joint Staff	Virage Inc.	6	25
IT06.90	Optimized Data Environment for NetCentric Operations (ODEN)		■	■	■						DISA	TIMMES, Inc.	6	26

History of Coalition Warrior Interoperability Demonstration 26

Abbreviations and Acronyms, inside back cover

IT01.01
Compartmented High Assurance Information Network

1. CROSS-DOMAIN DATA SHARING ● 3. INTEGRATED OPERATIONS ● 4. INTEGRATED LOGISTICS ● 5. INTEGRATED PLANNING ●

■ A Multi-Compartmented Windows Environment

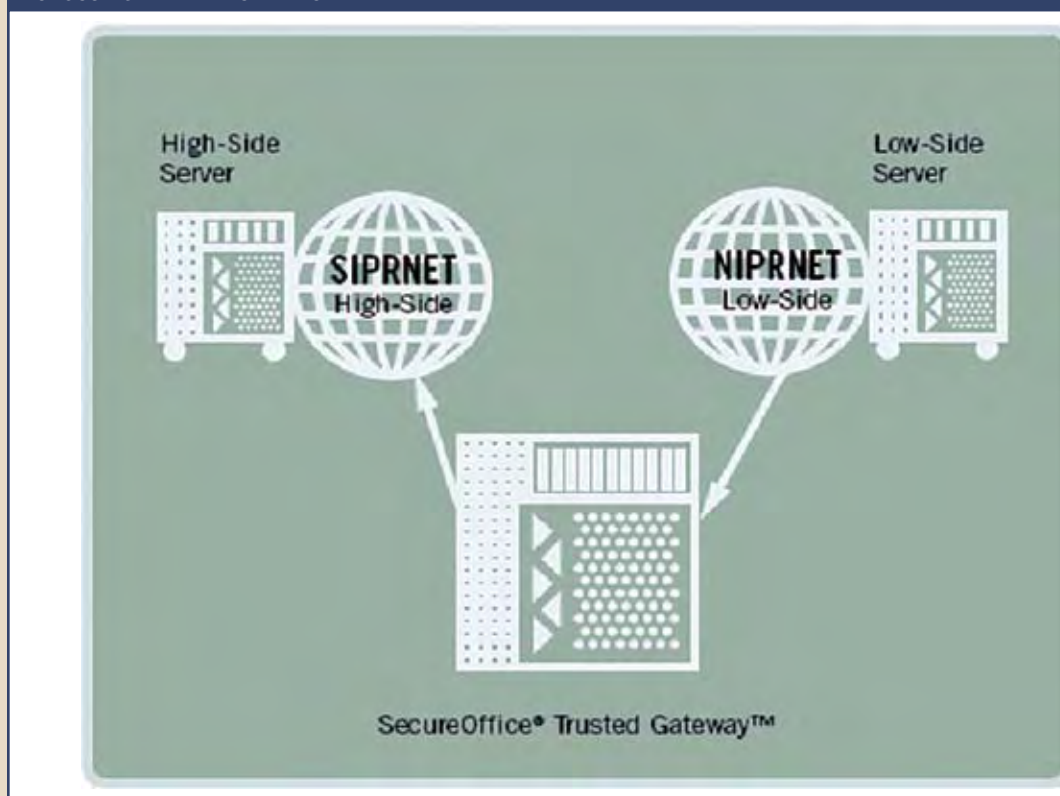■ Modeled on an open Service Oriented Architecture

■ Secure COTS-based solution

SPONSOR: USNORTHCOM
DEVELOPER: Raytheon
CONTACT: John Milford,
john_a_milford@raytheon.com

CHAIN, a solution not a product; a framework for information sharing; windows-based solution for multi-Compartmented secure interoperability in Joint and Coalition Operations; Microsoft Windows-centric SOA (Service Oriented Architecture); highly scalable; interoperable with non-Windows platforms

SERVICES FOR CWID 2007
■ Email
■ Collaboration
■ Web access
■ Text chat
■ File sharing
■ Secure Voice/Video

INFORMATION SECURITY
■ Encryption
■ Digital signatures
■ Content scanning

EFFICIENCY
■ Less infrastructure
■ Fewer people
■ Better communication
■ Less training

SECURITY
■ Enhances information sharing
■ Reduces possibility of unauthorized information
■ Simplifies information exchange with peers

IT01.05
Trusted Gateway System Guard

1. CROSS-DOMAIN DATA SHARING ●

SPONSOR: US Air Force
DEVELOPER: US Air Force
CONTACT: Marco Deluna
marco.deluna@lackland.af.mil

TGS Guard, provides a secure one-way transfer of data from one network to another network of higher classification or sensitivity level.

Using the TGS, an organization can electronically move large quantities of practically any type of data (e.g., imagery, maps, documents, e-mail, databases, etc.) from one network to another.

Data of any format or from any operating system, UNIX or Microsoft, can be transferred using the TGS Guard.

IT01.17

Cross Domain Collaborative Information Environment / Collaboration Gateway

1. CROSS-DOMAIN DATA SHARING ● 2. INTEGRATED INTELLIGENCE ● 3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●
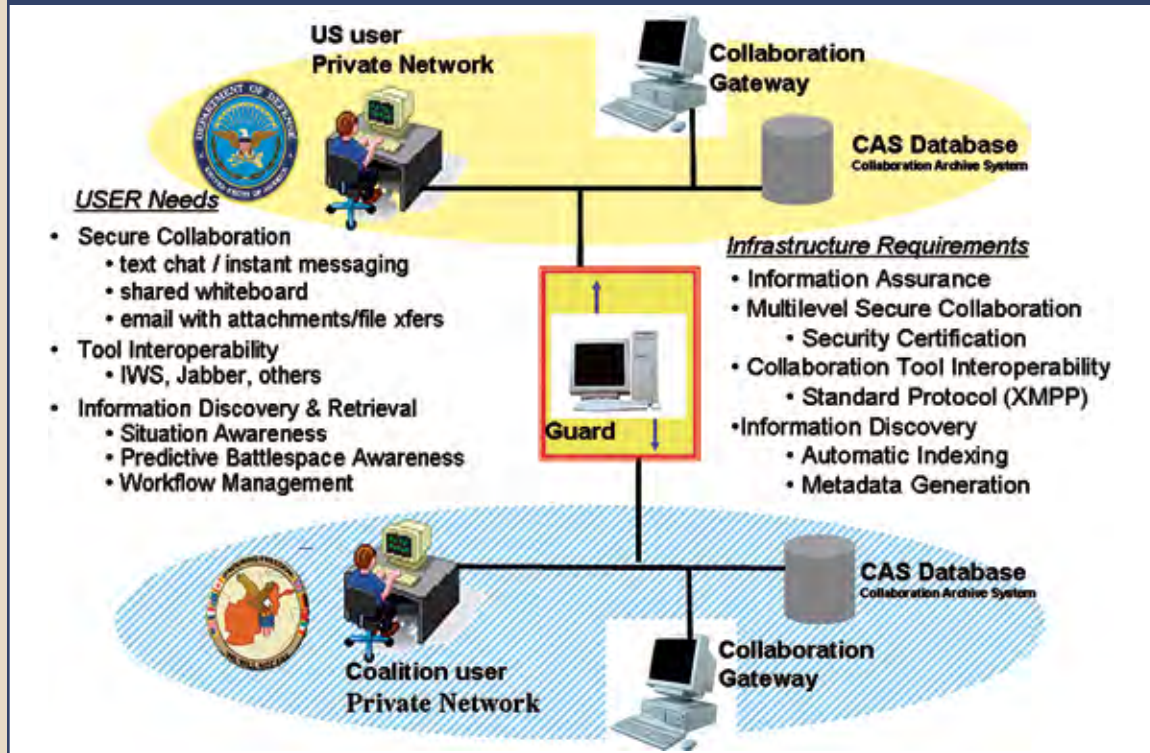
USJFCOM and the FBI team with Air Force Research Laboratories (AFRL) to enhance common Information Technology (IT) infrastructure supporting a unique Multi-Level Security (MLS) Information Sharing Environment (ISE).

CDCIE/CG is an umbrella program encompassing many Small Business Innovative Research (SBIR) initiatives addressing needs for MLS collaboration, interoperable collaboration tools, ISE discretionary access and information discovery.

IT01.28

NET/X eToken Security System, Deployable Communications System

2. INTEGRATED INTELLIGENCE ●

NET/X is a USB platform that, when connected to any Intel/Windows based computer, converts the workstation or mobile device into a terminal.

The NET/X device converts the existing network architecture to an integrated functional network, knocking down the "stovepipes" of information access, then back to its original state when disconnected.

The NET/X token will also allow users to connect to any workstation with internet connectivity anywhere, providing a secure terminal "tunnel" reaching back to IT Centers. NET/X establishes a proprietary VPN to the remote gateway. Inside the NET/X terminal, a connection to the remote NET/X Server is established using SSL or other encryption. The connection is then made to the target platform on the other end.

In its most common mode of operation, the user (at laptop) will be in a "read only" mode for data/graphics/text on the server.

IT01.43
Mobile Forces Solution - Subnet Relay

1. CROSS-DOMAIN DATA SHARING ●
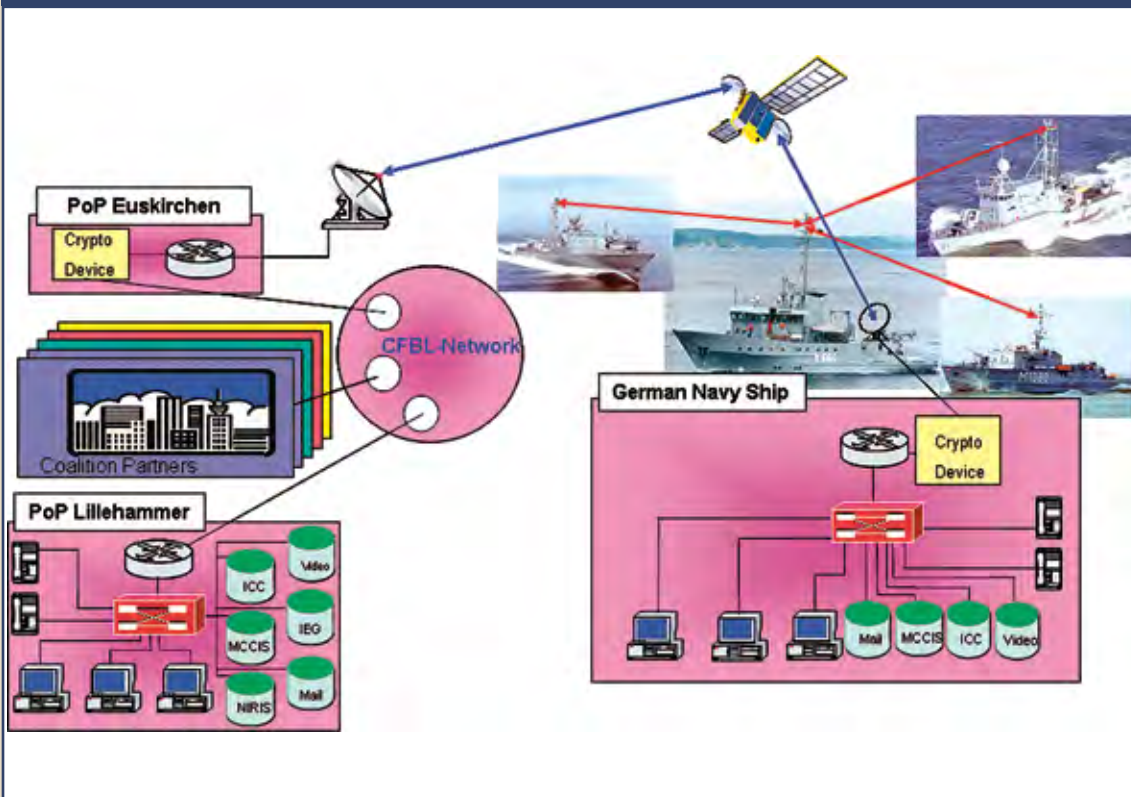
SPONSOR: Germany
DEVELOPER: T-Systems Enterprise Services GmbH
CONTACT: Gerhard J. Webler, +49 (228) 709.38204, gerhard.webler@t-systems.com; CDR Dirk Siebenmarck, +49 (4421) 68.5268 dirk.siebenmarck@bundeswehr.org

CWID Objectives Met: A distributed IP-Infrastructure with secure broadband satellite communication to ships and secure Subnet Relay via HF/UHF and DVB-T in order to provide data exchange among multiple applications such as MCCIS, ICC, eMail, ERP-System, VoIP and Video Conference

Provides: Maritime, Air and Joint C2 Services

Status: Practise proofed running demonstrator with experimental SubNet Relay functionality

IT01.54
Collaborate-Access-Browse

1. CROSS-DOMAIN DATA SHARING ●
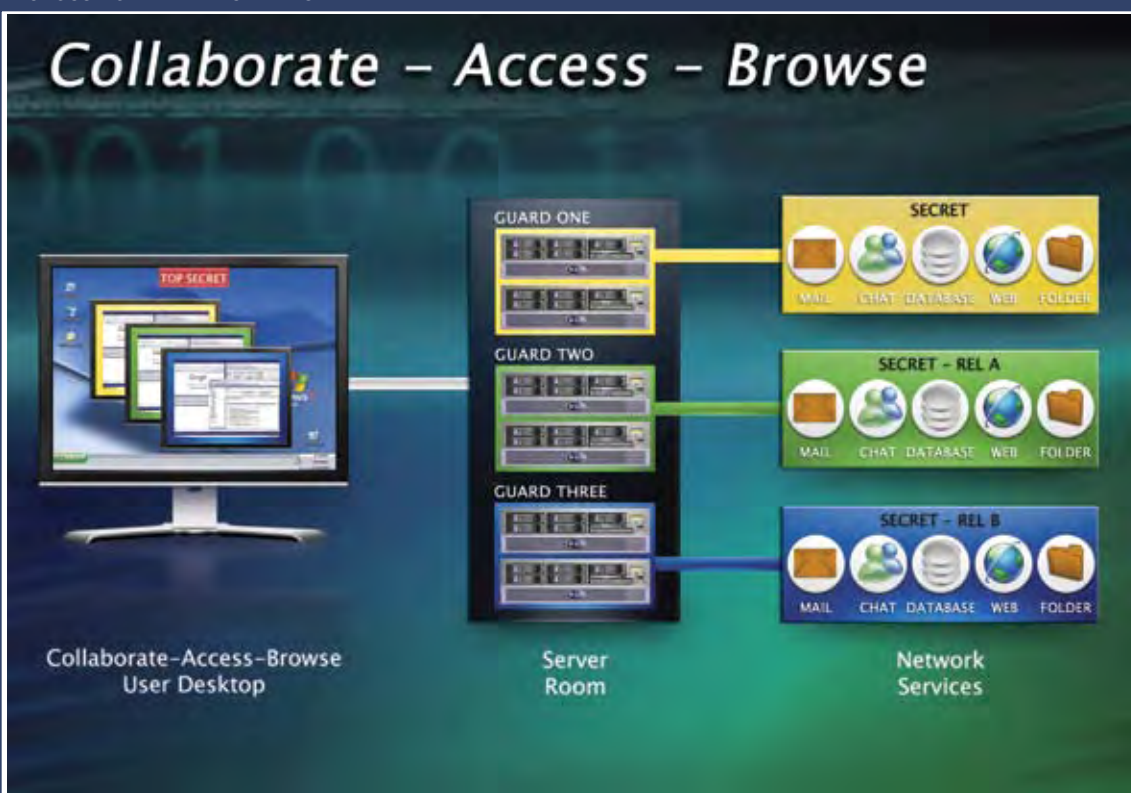
SPONSOR: NSA
DEVELOPERS: Concurrent Technologies Corporation, Essex Corporation, Tresys Technology
CONTACT: Cynthia Ameter 1.410.854.5150, cnameter@missi.ncsc.mil

CAB:
■ Reduces amount of desktop hardware to access networks
■ Designed to allow access from a higher classification to lower security domains
■ A competitively priced guard
■ Requires only server room hardware (appx. 1/2 rack)
■ Client is supported by Windows 2000 or newer platforms
■ Supports lower domain web browsing, e-mail, Office applications, databases, etc.
■ Blocks viruses and malicious code from the low-side network
■ Blocks transfer of classified information from the high to the low-side network
■ Supports up to 200 users on a single guard instance
■ Servers built on NSA SE Linux
■ Has a modular software design to meet specific mission needs
■ Will be certified for Top Secret and Below Interoperability, fall 2007

IT01.55
# Assured File Transfer

1. CROSS-DOMAIN DATA SHARING ●

AFT securely transfers high-risk complex files bi-directionally between domains of varying security classifications. AFT "cleans" files, removing malicious, hidden, and inappropriate content. For example, upon sending a Word, Excel, or PowerPoint file a user sends other information such as name, IP addresses, and previously deleted content. Cropped pictures can be un-cropped revealing parts not meant for viewing. AFT removes this information before sending the file.

AFT transfers files without revealing sensitive information while retaining native formats, has no impact on client machines, can be used as a policy enforcement tool and a desktop cleaning tool for High-Side users. AFT provides machine-to-machine capability and interoperates with any High-Side workstation supporting a modern browser.

IT01.56
Dual Diode Secure (One-Way) Cross Domain Data Transfer System

1. CROSS-DOMAIN DATA SHARING ●
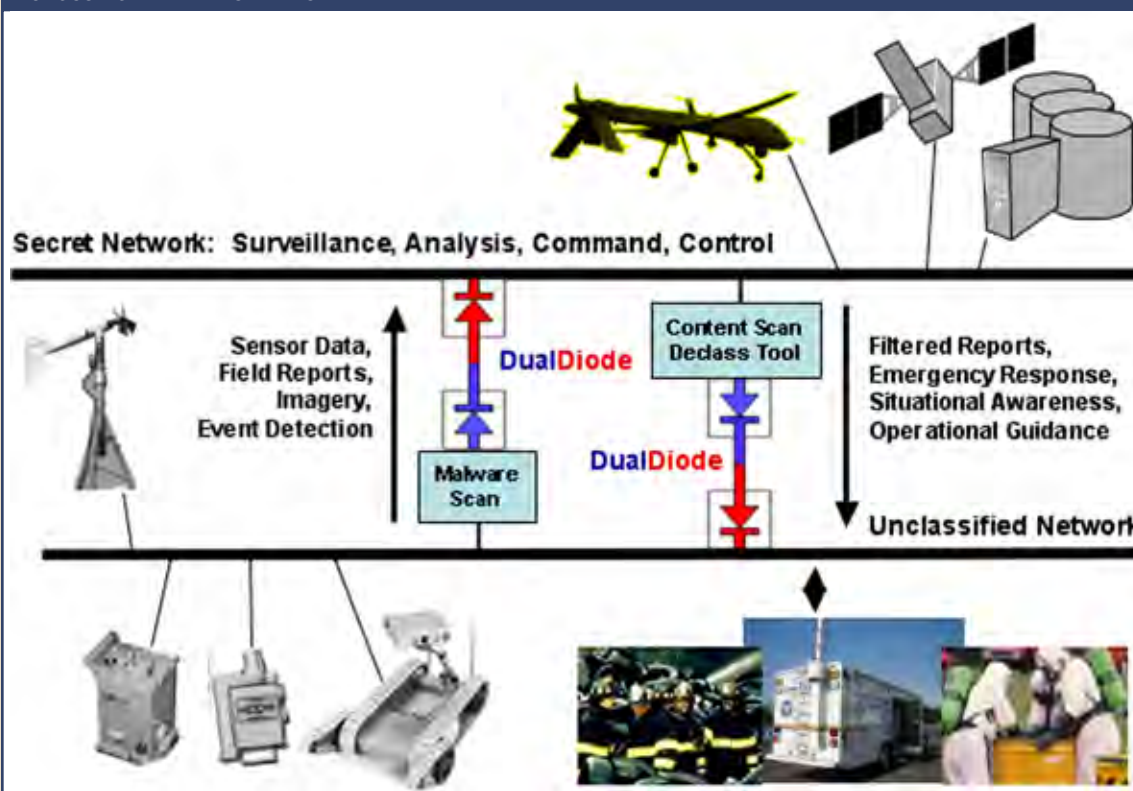
The Dual Diode provides a one-way real-time data link between isolated network security domains that is certified, accredited, and deployed throughout DOD and the U.S. intelligence community.

The Dual Diode consists of a pair of custom fiberoptic network interface cards (send-only and receive-only) installed in host computer platforms on separate networks. Hardware enforces high throughput forward data flow (155 Mbps) and denies backward data flow.

In CWID trials, the Dual Diode is integrated with content scanning software to provide cross domain data transfer solutions in upguard, peerguard and downguard configurations. Content scanning includes anti-malware for upguards, and human review declass tools for downguards.

IT01.61
INTEGRITY Secure Workstation

1. CROSS-DOMAIN DATA SHARING ●
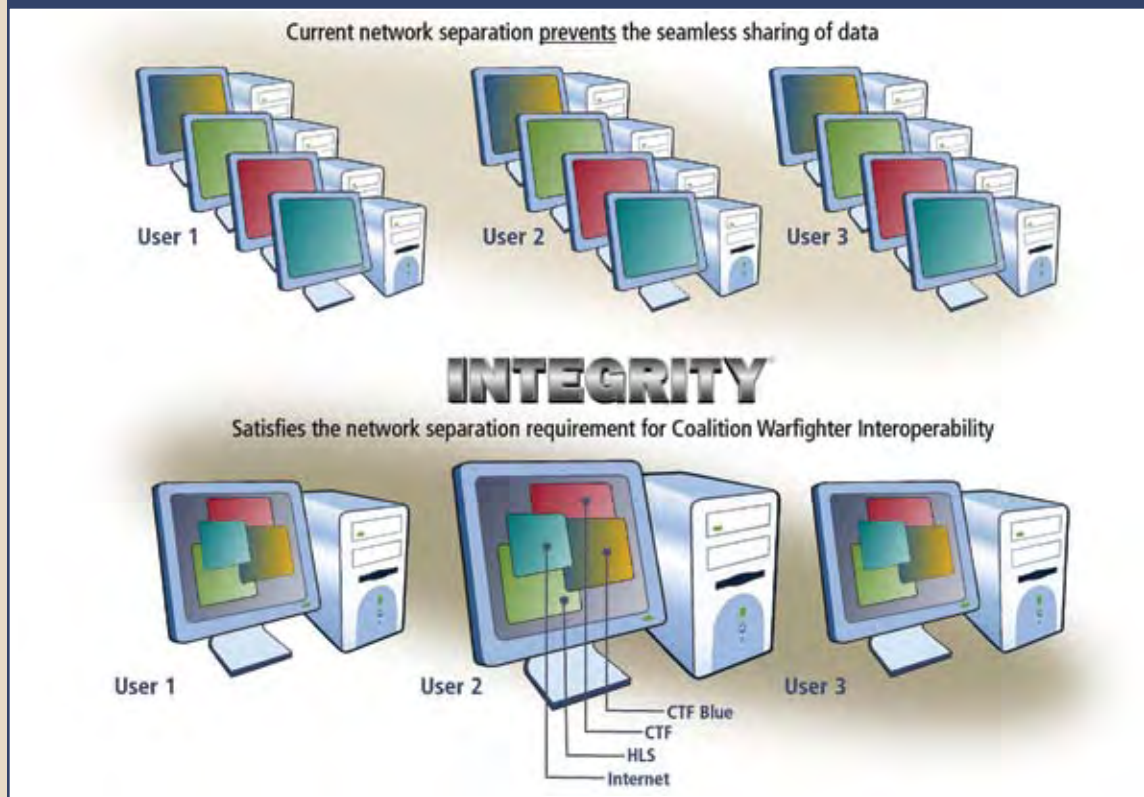
Current network separation prevents the seamless sharing of data

User 1 | User 2 | User 3

INTEGRITY

Satisfies the network separation requirement for Coalition Warfighter Interoperability

User 1 | User 2 | User 3

CTF Blue
CTF
HLS
Internet

Information Technology is as important as a weapon system in the war on terror. Protecting it is paramount.

As the Operating System provider on JSF and F-22, INTSecWS extends the safety and security attributes of a weapons system to the desktop, allowing the seamless sharing of information across multiple security enclaves.

An assured separation kernel that enforces information flow control policy is fundamental to operations in a Cross Domain environment. INTEGRITY-178B is the only operating system technology undergoing EAL 6+ penetration testing at the NSA.

INTSecWS ensures that Windows and Linux applications are isolated, protected, and guaranteed and is recognized as the only capabilities-based microkernel that can provide guaranteed resource availability.

IT01.63
Coalition Assured Sharing Environment

2. INTEGRATED INTELLIGENCE ●

Coalitions Assured Sharing Environment (CASE)

STRATEGIC | MISSION SYSTEMS

HIGH ASSURANCE PLATFORM (HAP) | UNCLASSIFIED | CWID BACKBONE | CASE SERVER

S//NOFORN
S//Releasable

MOBILE | TACTICAL/ GARRISON

The General Dynamics CASE provides an enterprise solution to:

FRONT-END
1. Utilize information from different Communities of Interest (COIs), and Security Domains on a single High Assurance Platform (HAP).

BACK-END
2. Provide access to information and enterprise applications based on COI membership.

3. Move information between Security Domains via an integrated certified and accredited cross-domain Guard and workflow toolset.
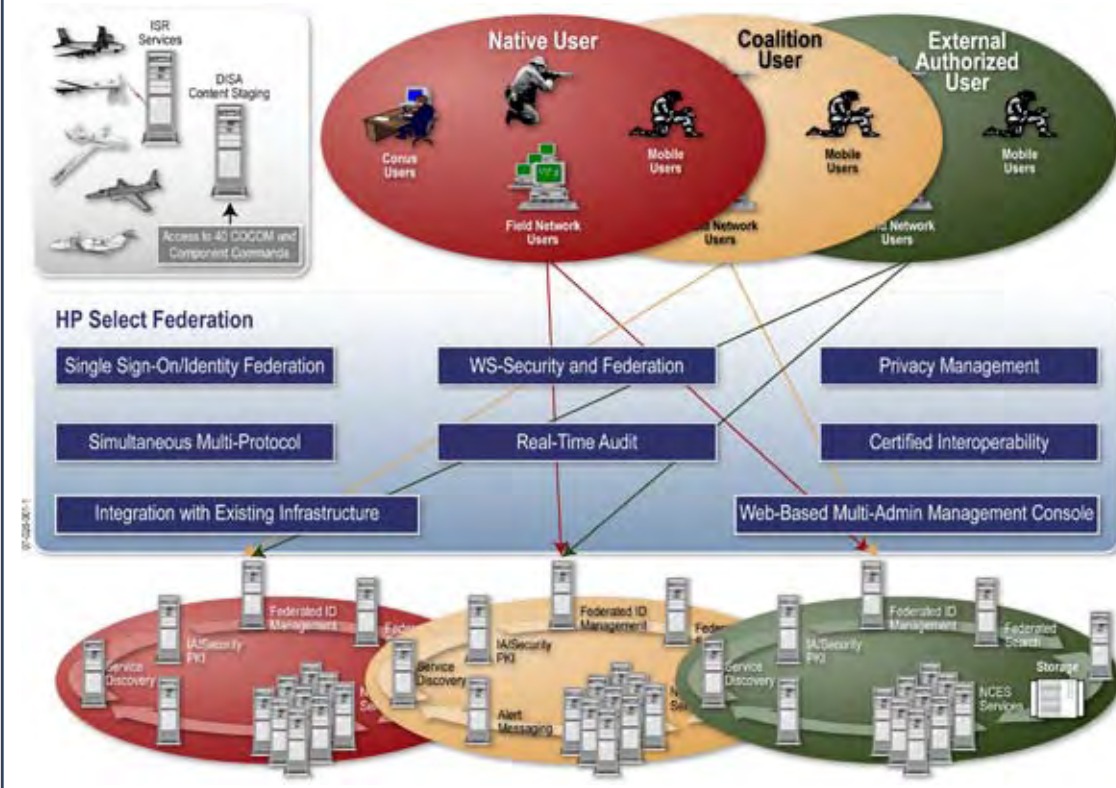
MANAGEMENT INFRASTRUCTURE
4. Change access policy and COI membership to control data access dynamically.

IT01.86
Federated Identity Management System

1. CROSS-DOMAIN DATA SHARING ●

Coalition warriors require access to information in different security domains. Current manual processes to grant access to required information create inefficiencies that impact the mission.

FIdMS addresses inefficiencies and complications of network identity management for multiple agencies among coalition warrior partners. It allows users to "link" elements of their identity between accounts without centrally storing identity information.

THIS INFRASTRUCTURE:

■ Provides a superior online experience, personalization, security and control over identity information

■ Enables IT managers to easily and securely provision accounts and resources

■ Enables C/S/A and partners to efficiently create trusted relationships by leveraging existing identity systems, allowing realization of mission objectives, while performing securely and at a lower cost

IT01.87
Federated Security

2. INTEGRATED INTELLIGENCE ●
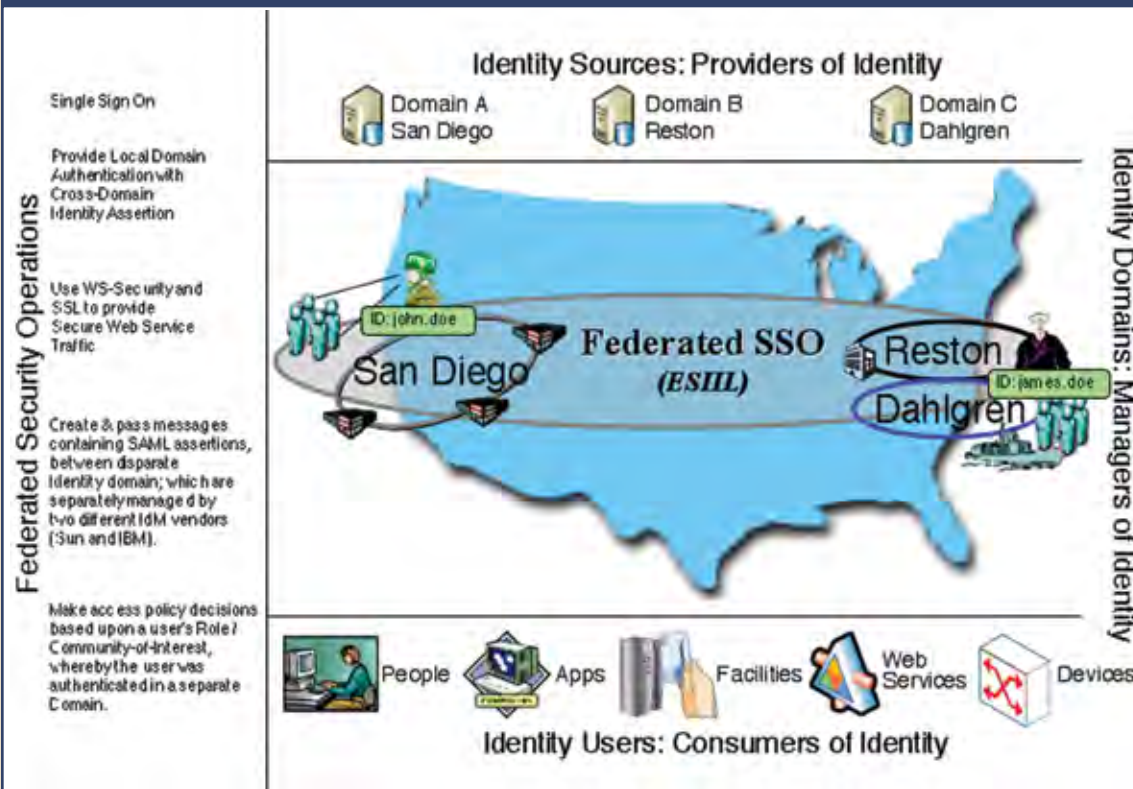
The FS system addresses one of the most difficult aspects of implementing a Service Oriented Architecture (SOA) environment, authentication and authorization to distributed resources.

The FS system demonstrates the ability to perform cross-domain identity management and single sign-on using COTS identity management products in a SOA environment.

The SAIC team developed a solution using COTS products. This is particularly a challenge to DOD and DHS because of the multitude of different networks that exist at the federal, state, and local level.

The most useful capability that it would give a user is the ability to sign on to one network and access information on a different network. A user would logon one time and then access resources on multiple networks as if they were all on the same network. These resources may be files, web pages, or application software.

IT02.06
Italian Navy Maritime Command & Control Information System

2. INTEGRATED INTELLIGENCE ●
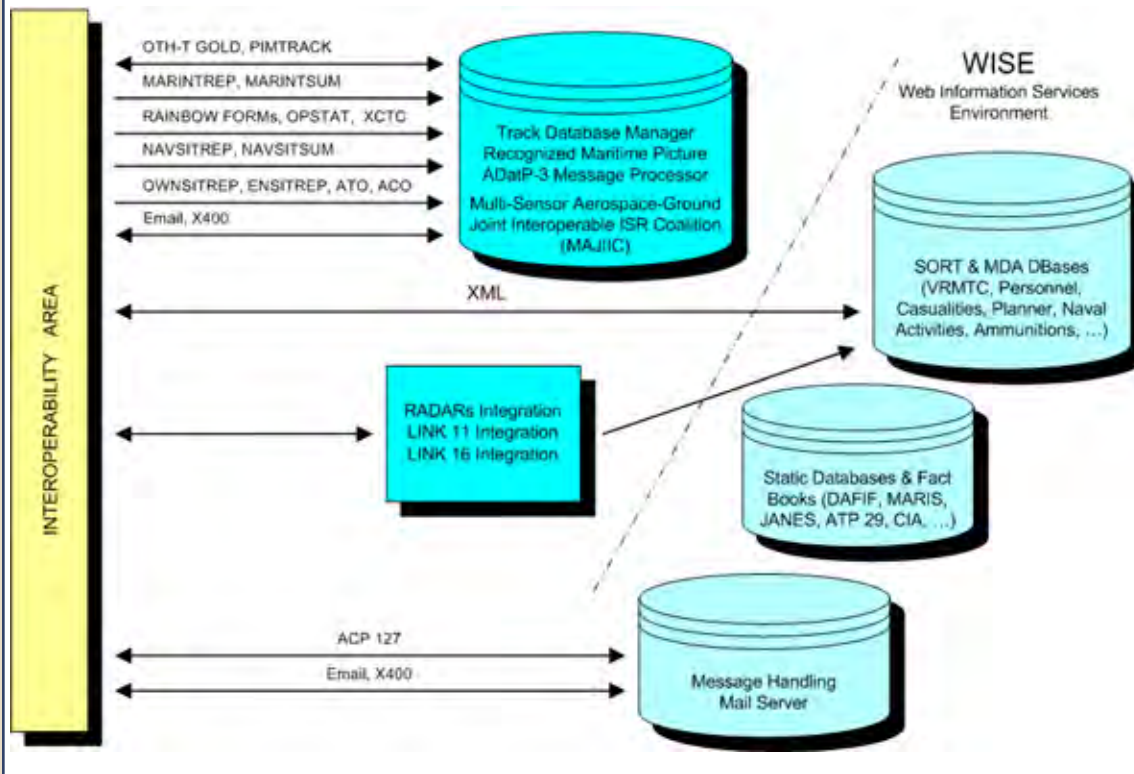
SPONSOR: Italy
DEVELOPERS: NATO ACT, Engineering Ingegneria Informatica S.p.A. Rome, IT
CONTACT: Lt.Cdr. Sergio Ciannamea, +39.06.3680.9334
ciannameas@marina.difesa.it

MCCIS-Italy v.5.2 has been developed and maintained to allow maritime commanders and staffs to automatically acquire and maintain large quantities of information for display and analysis.
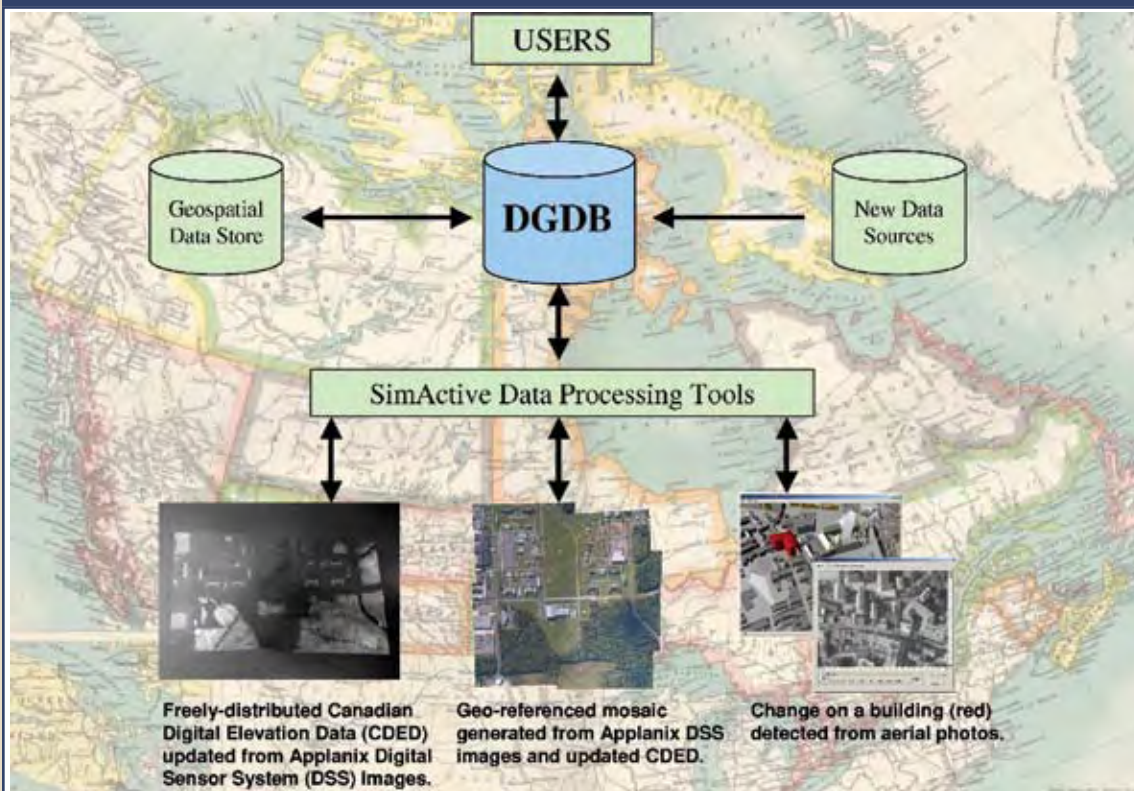
The trial electronically processes multiple source data, displays the information in various Command and Control (C2) applications and provides users with the ability to manipulate the data to assist strategic, operational and tactical commanders (and staffs) in decision making processes.

MCCIS-Italy v.5.2 provides RMP, MTF, SORT, MDA data and e-mail exchange, testing the capability of the new release to be fully interoperable and integrate with other US CWID 2007 C4I systems.

IT02.16
Deployable Geospatial Database

2. INTEGRATED INTELLIGENCE ●

Freely-distributed Canadian Digital Elevation Data (CDED) updated from Applanix Digital Sensor System (DSS) Images.

Geo-referenced mosaic generated from Applanix DSS images and updated CDED.

Change on a building (red) detected from aerial photos.

SPONSOR: Canada
DEVELOPER: MCE, SimActive
CONTACT: Mario Beauchesne, 1.613.992.7727,
beauchesne.mc@forces.gc.ca

DGDB is a data model used to support mission-specific in-theater operations. It's a new approach developed under ArcSDE (Shared Data Environment) to manage, share and disseminate data at theater-wide level. This model is based on the U.S. Theatre Geospatial Database (TGD).

DGDB also integrates SimActive technology, developed in collaboration with DRDC Valcartier. It allows the automatic integration of 2D imagery, such as aerial photos, with 3D data (e.g. Digital Elevation Models).
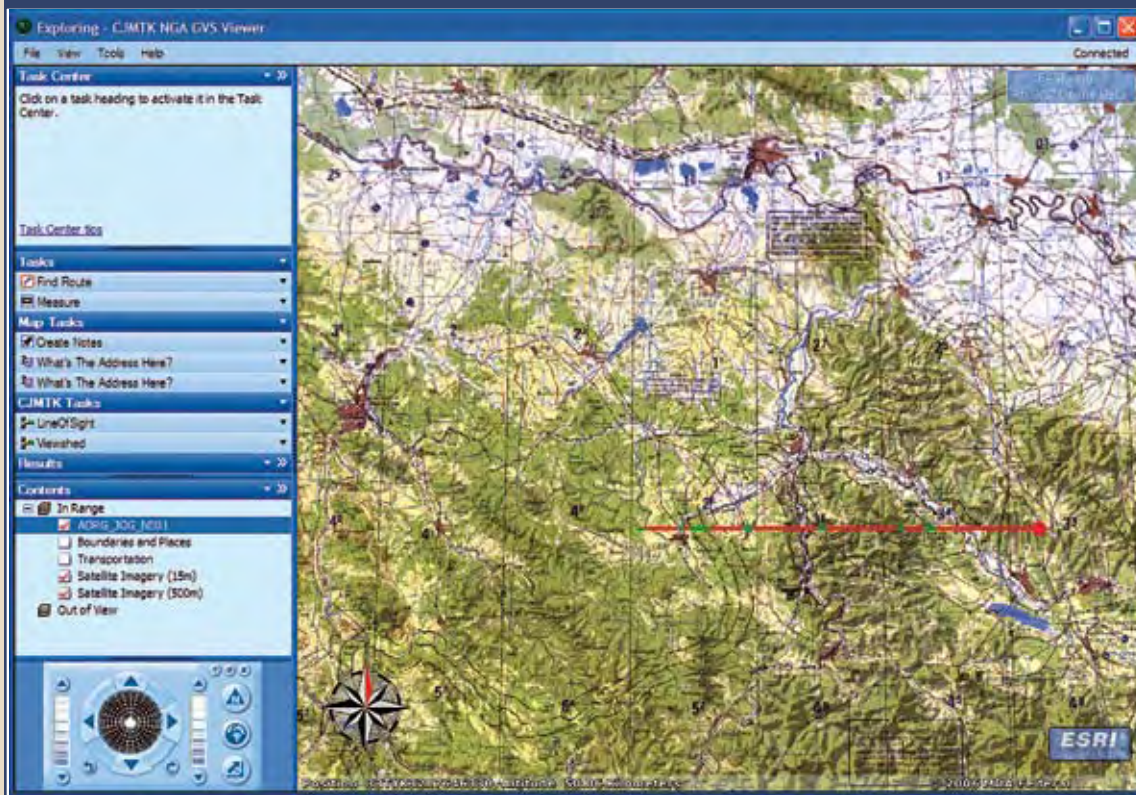
The technology can register imagery with 3D data for the creation of precise orthophotos. It can also detect 3D differences and update 3D data to track structural changes or improve the quality of an existing 3D data set.

IT02.21
Commercial Joint Mapping Toolkit

2. INTEGRATED INTELLIGENCE ●

CJMTK is the recommended geospatial software toolkit for the DOD Command and Control Intelligence (C2I) community to perform situational analysis (such as determining troop locations which will yield a position of advantage over an enemy, or identifying the most efficient routes for moving troops and equipment).

In addition, the system provides map data in an application-ready format, allowing systems to see and use map data without software compatability issues.

These capabilities employ the Web, provided in accordance with accepted standards. This allows other client systems, which support these standards, to use the systems' tools for conducting analysis and viewing data.

IT02.37
Rapid Force Warning

2. INTEGRATED INTELLIGENCE ●

RFW will demonstrate the ability to rapidly deploy, setup and configure missile early warning capability in support of operations at immature or austere sites where communications infrastructures or permanent facilities have not been established. RFW enables the sharing of missile warning data with coalition forces and has the unique ability to tailor reporting of ballistic missile threats in the region utilizing a rule-based gateway.

RFW offers commanders a tool to rapidly establish sharing of missile warning data releasable to coalition forces. RFW utilizes a pay-by-the-packet methodology—paying only for the amount of data being processed while maintaining a small footprint. This rapidly deployable and low cost capability can enhance passive or active defense, attack operations and battle space situational awareness.

IT02.57
Automatic Ingest Mosaic Mapping System

2. INTEGRATED INTELLIGENCE ●
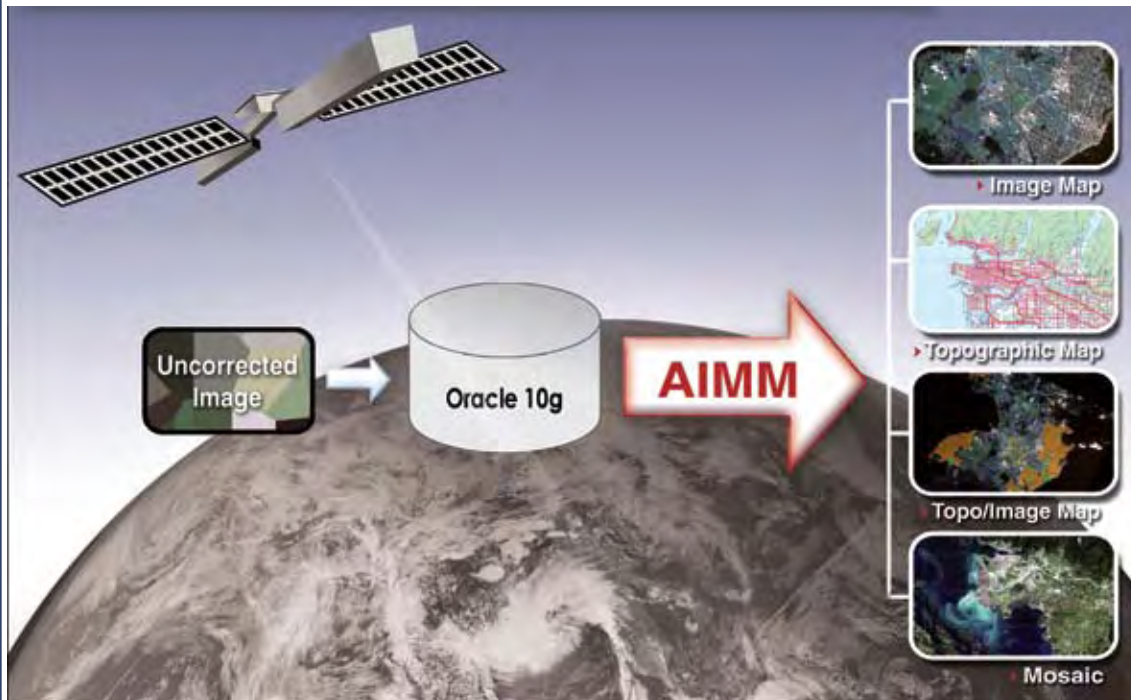
SPONSOR: Canada
DEVELOPER: PCI Geomatics
CONTACT: Bonnie Harris,
harris@pcigeomatics.com
1.819.770.0022 (X323)

PCI Geomatics' AIMM is a cost-effective and time efficient system for transforming geospatial data and imagery into critical decision support information.

An automated production environment, AIMM can ingest a wide variety of satellite imagery, automatically determine the satellite type, correct the raw imagery to remove distortions, and insert this imagery into an Oracle 10g database.

Operators are able to insert and query available imagery pertaining to their area of interest via a web interface, based on any or all of the following options: location, time of acquisition, resolution, and sensor type. This intuitive system automatically responds and notifies the operator by sending the requested imagery via FTP or email. This system offers a vast variety of possible output formats, (e.g. a geocoded image in NITF format, GeoTiff, JPEG, a mosaic product made up of multiple images, or a finished map product).

IT02.88
AdLib

2. INTEGRATED INTELLIGENCE ●
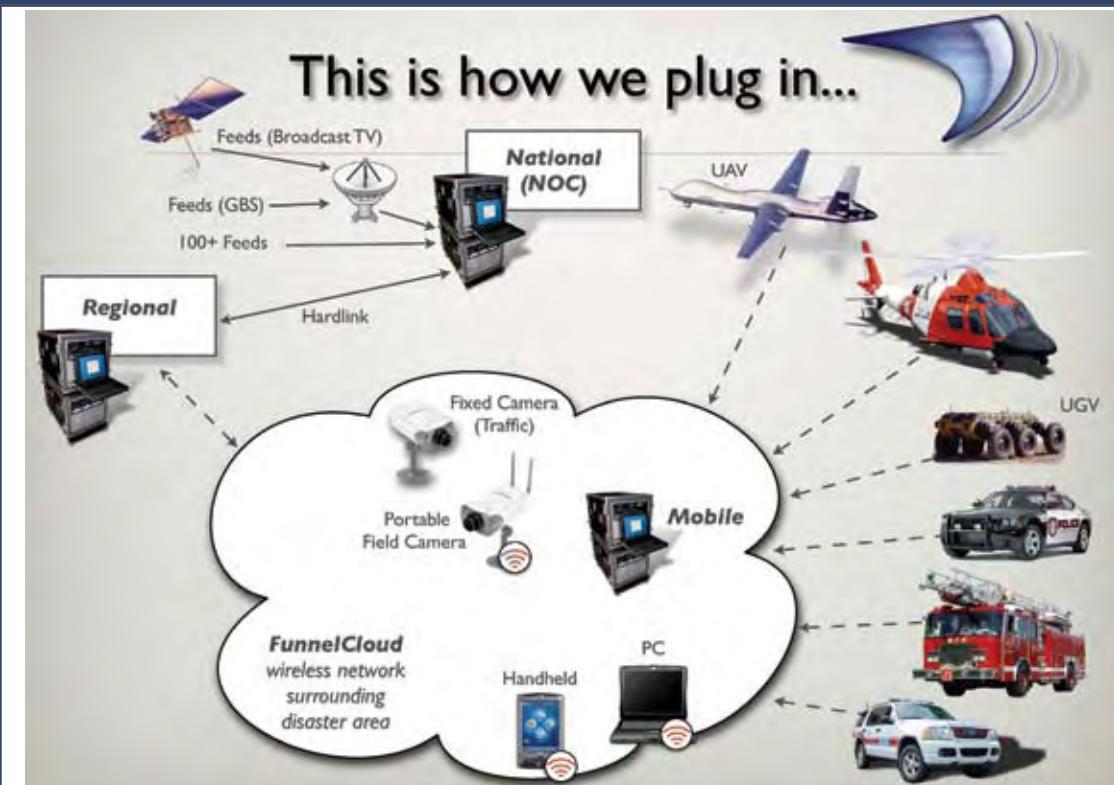
SPONSOR: USNORTHCOM
DEVELOPER: EchoStorm, Inc.
CONTACT: William Ormsby,
william.f.ormsby@navy.mil

AdLib captures and stores (60-to-90-days) analog and/or digital video and respective metadata, enabling intelligent location, access/control, and alerting of fixed and mobile video sources such as Unmanned Aerial Vehicles (UAVs). As a Web Services solution, AdLib can be integrated into video data and sensor feeds from multiple collection platforms and mobile/portable video and sensor data capture sources.

AdLib has been integrated with Falconview, ESRI, Google Earth, Cursor on Target, C2PC and Federated Search NCES applications, and works with operational UAVs. It encrypts and compresses video/sensor data feeds, and applies Transport Layer Security to redistribute context-specific video/sensor feeds to operators using various computer/communication devices.

Video and sensor feeds are distributed over low bandwidth to warfighters in Iraq from the operations center in 18 seconds using a Java messaging applet.

IT03.09
Global Personnel Recovery System

2. INTEGRATED INTELLIGENCE ● 3. INTEGRATED OPERATIONS ● 4. INTEGRATED LOGISTICS ● 5. INTEGRATED PLANNING ●

Real Time Tracking, Real Time Command and Control

SPONSOR: USJFCOM
DEVELOPER: Innovative Solutions International
CONTACT: Richard W. Cole, rwcole@isicns.com, 1.703.626.6756

GPRS is a two-way messaging and tracking system designed to link mobile and fixed surface users, airborne users and command/control elements at any distance. GPRS provides flexible, nearly instantaneous communications and location via satellite. It can rapidly group and regroup response teams to meet changing needs.

GPRS provides DOD and civilian search and rescue personnel with the capability to quickly identify and accurately locate people in need of rescue services anytime, anywhere in the world.

GPRS can enhance responsiveness across civil and other government organizations, providing aircraft and vehicle tracking, remote sensing, and command and control of rescue and first responder organizations.

GPRS encompasses user devices, satellites, earth stations and command and control infrastructures at multiple levels.

IT03.14
Coalition Secure Management and Operations System

3. INTEGRATED OPERATIONS ● 6. INTEGRATED COMMUNICATIONS ●
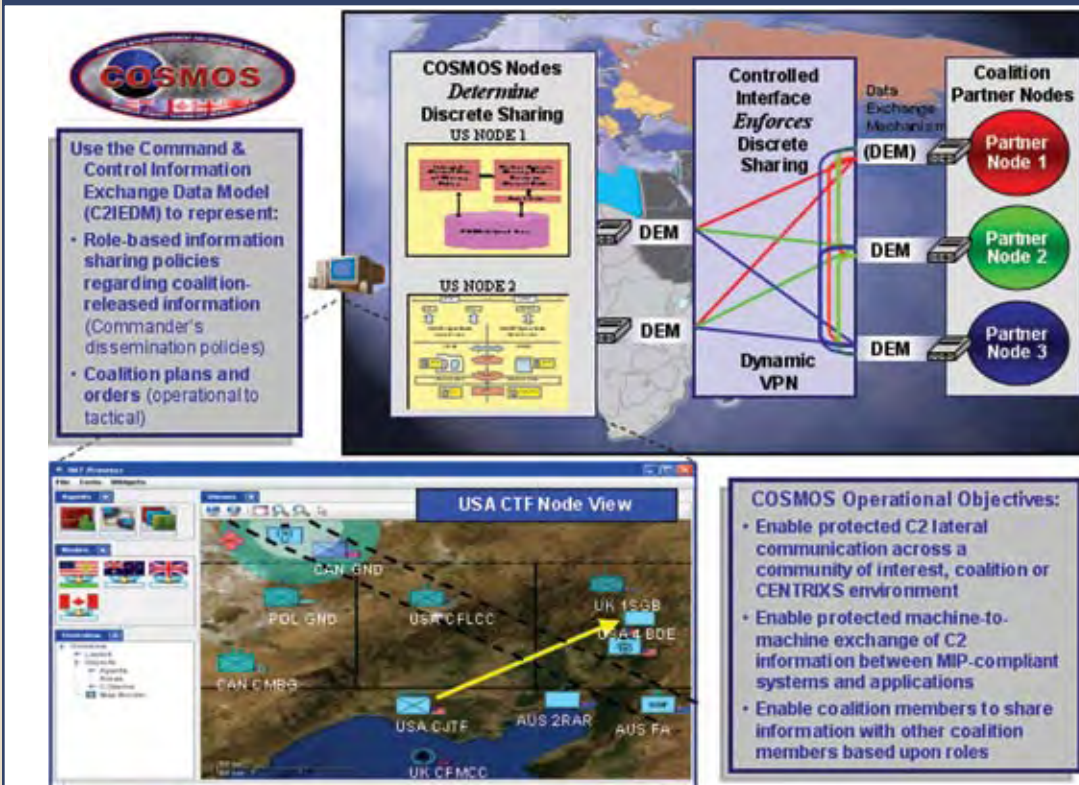
SPONSOR: OSD, USEUCOM, USPACOM, DISA
DEVELOPERS: DISA, NSA, CDM
CONTACT: Peggy Palmer, palmerp@eucom.mil

COSMOS, an ACTD, enables protected and selected sharing of command and control (C2) information among coalition partners on a single coalition network leading to more rapid and decisive operations by:
■ Automating information management
■ Improving C2 operations support
■ Enhancing C2 information exchange security
■ Data to the right coalition partner based on role, location, and need to share
■ Implements the Multilateral Interoperability Program (MIP) C2 Information Exchange Data Model (C2IEDM) and Data Exchange Mechanism (DEM).
COSMOS EXCHANGES:
■ Common Operational Picture inputs (locations, tracks, status)
■ C2 information (distributes and displays orders and tasks)

COSMOS will deliver a critical operational capability soon and reduces the risk for Multinational Information Sharing (MNIS) and service transition/integration capabilities.

IT03.22
Scalable Mesh Networks

2. INTEGRATED INTELLIGENCE ● 3. INTEGRATED OPERATIONS ●

SPONSOR: US Navy
DEVELOPER: OrderOne Networks
**CONTACT:** David Davies, david@OrderOneNetworks.com

OrderOne Networks provides a truly scalable Mobile Ad Hoc Network (MANET) protocol and a 3D network visualization tool that is linked directly into the network.

The MANET protocol can support 100,000's of nodes and may be installed on virtually any device from sensors to handheld radios to vehicles and aircraft.

The 3D network visualization tool was designed for boots-on-the-ground personnel who need instant network situational awareness, including the location of other nodes and their status, and also communication with them. It also enables instant historical review of network activity and node movements.

IT03.27
Integrated Information Management System

3. INTEGRATED OPERATIONS ●
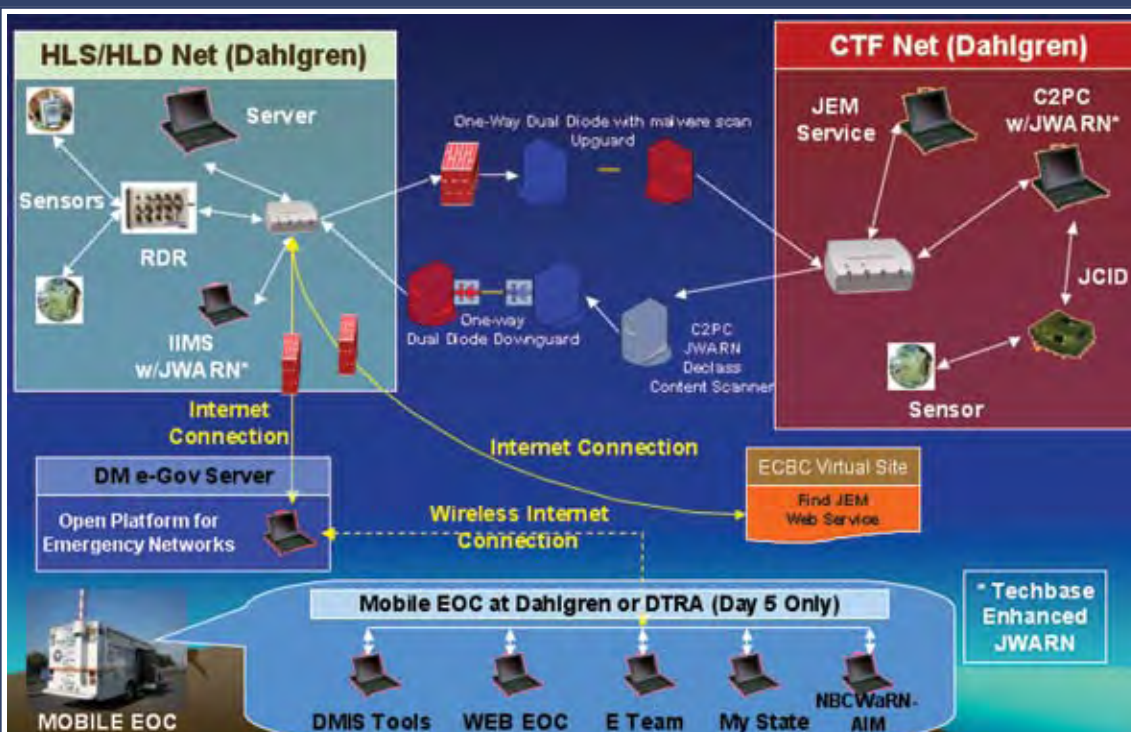
IIMS IS CURRENTLY FIELDED IN:
- ■ U.S. Pacific Command (USPACAF) in the Korean theater of operation, Osan Air Force Base
- ■ U.S. Central Command (USCENTCOM) in the Southwest Asia theater of operation, Port of Ash Shuaybah, Kuwait

SPONSOR: US Air Force
DEVELOPERS: US Army, US Air Force
CONTACT: Donald Macfarlane, 410.436.5876, donald.macfarlane@us.army.mil

IIMS is an integrated hardware and software network which includes display of detector data, event management, hazard prediction, and CBRN hazard messaging. IIMS is interoperable with DoD C2 Systems and Emergency Management Alert Systems.

IIMS will use a two-way guard for passing information both low to high and high to low and exchange alerts with a civilian mobile Emergency Operation Center (EOC). The EOC shares alerts with Federal, State and Local agencies through Open Platform Emergency Networks (OPEN).

IIMS has evolved from the Restoration of Operations (RestOps) Advanced Concept Technology Demonstration (ACTD), Contamination Avoidance at Seaports of Debarkation (CASPOD) ACTD, and DTRA JSTO CBD Efforts.

IT03.30
Spatio-Temporal Analysis for Rapid Tasking

3. INTEGRATED OPERATIONS ●

SPONSOR: US Air Force
DEVELOPER: The MITRE Corporation
**CONTACT:** Nikhil Kalghatgi, nikhil@mitre.org, 1.781.271.4786

START demonstrates how a system providing insight into automation enables warfighters to dynamically replan Intelligence, Surveillance and Reconnaissance (ISR) assets with improved situation awareness (SA), confidence, and target coverage.

When an ISR asset is unexpectedly called upon, e.g. for a Time-Sensitive Target (TST), START provides the decision-making environment to dynamically modify the current ISR schedule. By partnering human interaction with an asset-target pairing optimizer, users can perform what-if analyses on asset re-tasking for dyanmic and highly effective ISR operations.

IT03.31
Coalition Infrared Data Processing

3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●
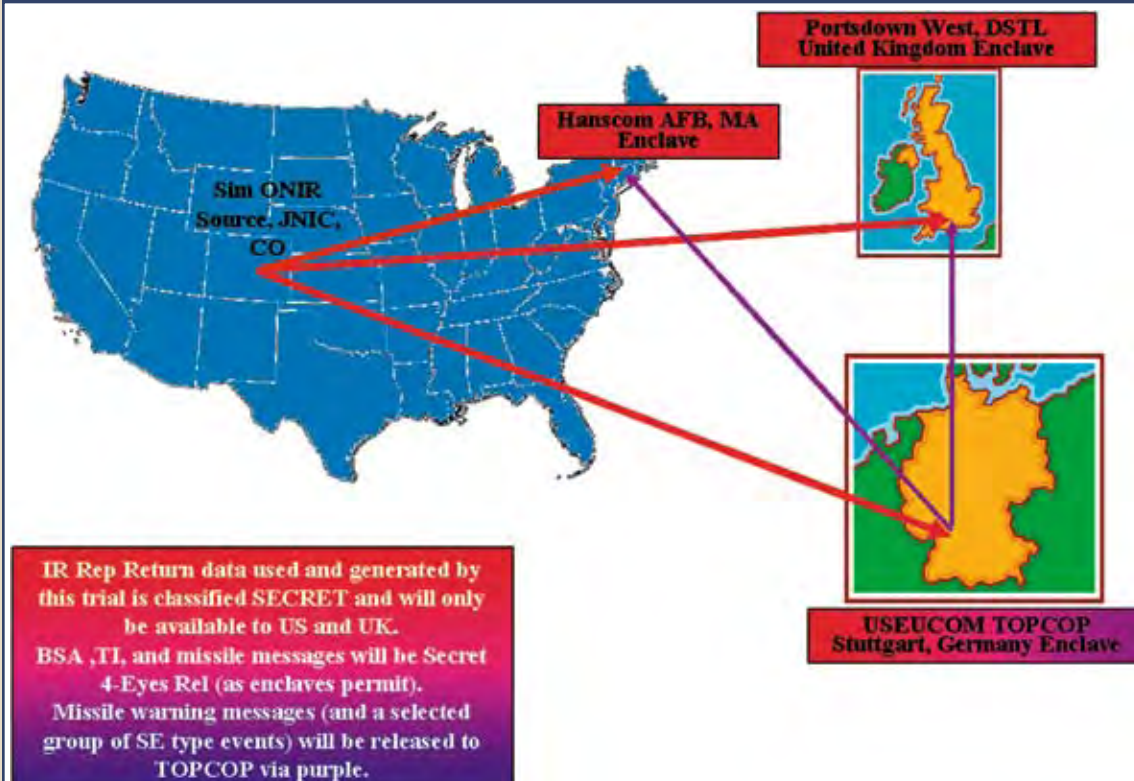
SPONSOR: US Air Force
DEVELOPER: Space and Missile Center, Missile Defense Agency
CONTACT: Capt. Christopher Michele, christopher.michele@buckley.af.mil, Kenneth Kowalski, kenneth.w.kowalski@aero.org

CIDP demonstrates use of overhead non-imaging infrared sensors to expand the missile warning function historically provided by the DSP system: battlespace awareness (battlefield activity and bomb damage assessment); indications and warning of changes in the battlefield (force redeployment and precursors to attack).

DSP/SBIRS
WARFIGHTER UTILITY
■ **Missile Warning:** Strategic early warning of enemy ballistic missiles

■ **Missile Defense:** Detection of enemy strategic and tactical missiles for missile defense and response

■ **Technical Intelligence:** Gather, identify and analyze heat signatures of missiles for intelligence fusion and analysis

■ **Battlespace Awareness:** Increased tactical situational awareness – tactical missile location and battle damage assessment

IT03.38
Collaborative Decision Aid

3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●

CDA is an integrated suite of web-enabled software applications, presented in a web portal environment, and accessed via web browser. CDA can be configured to support synchronous conferencing and information sharing using a variety of data sources. It provides access to users at different access levels and disparate locations via the Internet, NIPRNET, or SIPRNET.

CDA links decision makers in real-time to facilitate situational awareness "at a glance." Through a portal architecture, the CDA conferencing and decision support environment can be accessed simultaneously at all levels: Federal, State or Incident site.

Decision makers, operational staffs and first responders can rapidly attain an identical level of situational awareness and understanding, quickly formulating decisions based on the current emergency situation, using the applicable operational procedures, checklists and templates.

IT03.39
Command, Control, Communications, Computers and Intelligence Defense Joint System

3. INTEGRATED OPERATIONS ●
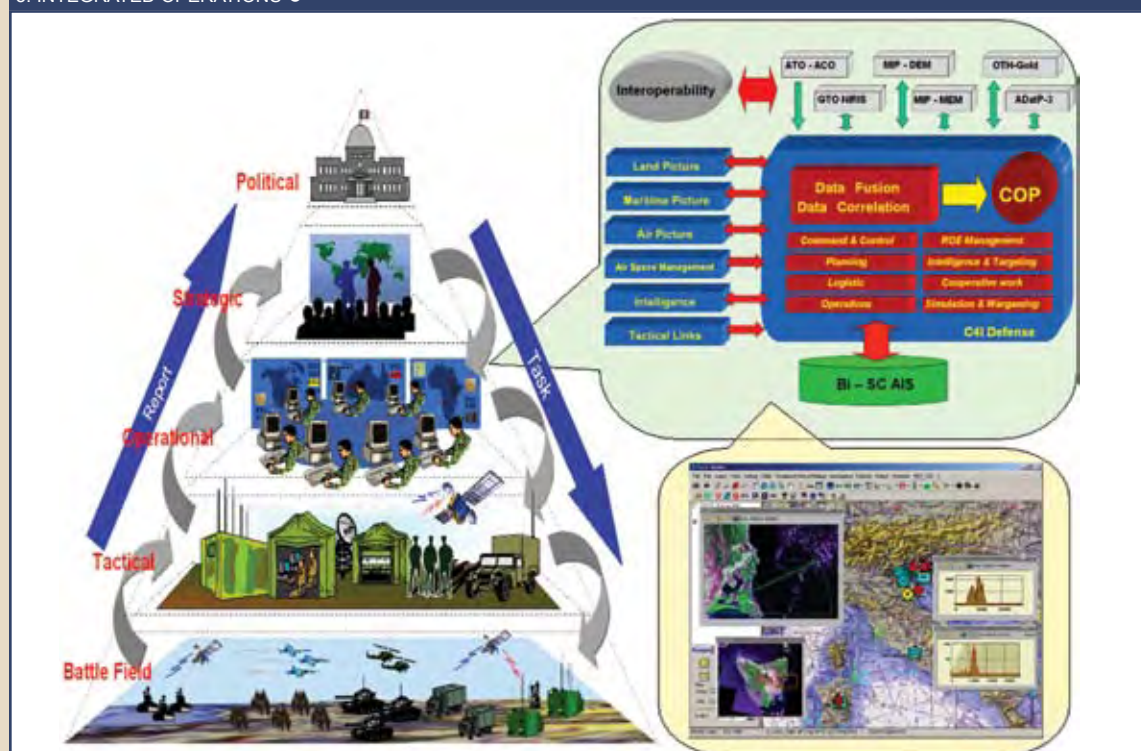
Italian C4I Defense joint system has been designed to provide top-level strategic capabilities, laying above the tactical functionalities offered by the C2 systems of each Service

The trial objective is to test data and information exchanging capabilities with other NATO/PfP/US, joint and single service C2 systems, by supporting high level C2 capability and COP exchanging.

C4I Defense joint system tests its capability of sharing COP in a multilateral environment, through formatted messages in OTH-Gold, ADatP-3 and USMTF 2000 standards.

Italian Joint Operation Headquarters and staff can share COP and improve their situational awareness in a multinational environment.

IT03.48
Air Support Operations Center with Close Air Support System

3. INTEGRATED OPERATIONS ●

SPONSOR: US Air Force
DEVELOPERS: US Air Force, US Navy
CONTACT: Blair Evens, blair.evens@langley.af.mil

The ASOC Gateway provides the capability to tie all Joint Tactical Air Controllers (JTACs) on the battlefield with digital network aircraft (Link 16/SADL). The CASS software itself, without the use of the gateway, has direct line-of-site digital communications with FA-18s, AV-8Bs, and F-16s.

This capability is being expanded to aircraft such as the A-10, B-52, and Network Enabled Weapons such as Small Diameter Bomb.

IT03.58
U.S. Coast Guard Information Sharing & Communications

3. INTEGRATED OPERATIONS ●
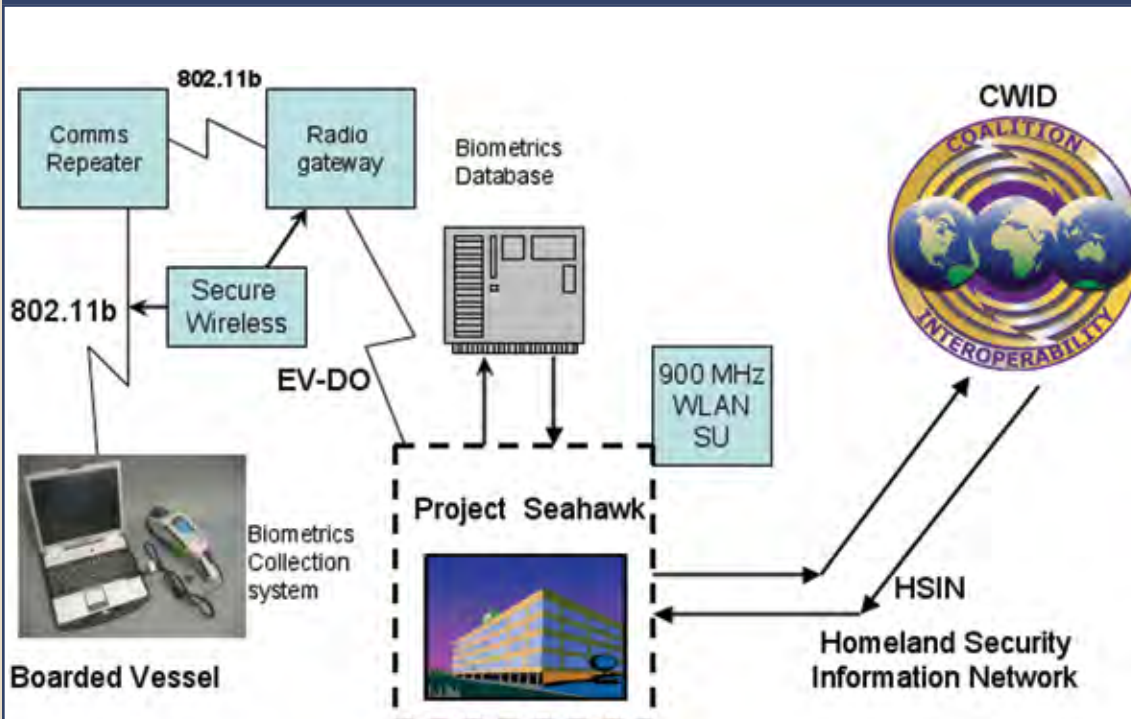
SPONSOR: US Coast Guard
DEVELOPER: US Coast Guard
CONTACT: Albert Hartberger, albert.w.hartberger@uscg.mil

USCG IS&C provides a rapid and secure means of communicating from vessels off shore to the local command center and anywhere. It solves a long standing problem maintaining communications with boarding teams. It works even when the boarding team is deep within a large ship.

It will also provide rapid and secure transmission of biometric data. A portable fingerprint scanner collects biometric data, downloads to a laptop and is securely transmitted via an encrypted wireless network to a command center. From there it can be passed to higher level operational commanders, other federal government agencies, state and local agencies. The data is then transmitted to a secure fingerprint database and the results are quickly sent back to the boarding team.

This trial will provide a substantial improvement in situational awareness to appropriate command and control entities through a net-centric community of interest (COI).

IT03.70
Coalition open Joint Operations Picture

3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●

COJOP IS A SOLUTION WITH AN ARCHITECTURE THAT INCLUDES:

- A presentation framework that is configurable and extensible
- A document repository that is replicated between sites
- An enterprise services architecture for web services
- Delivery of legacy applications via terminal services
- A Geospatial Information Service for pictorial display
- Collaboration through persistent Chat and event driven blogs

SPONSOR: UK
DEVELOPER: Fujitsu Services
CONTACT: Kevin Parry, kevin.parry@uk.fujitsu.com

CoJOP is the coalition deployment of openJOP that delivers the Joint Operations Picture (JOP) on the (UK) Defence Information Infrastructure (DII).

The trial's ability to generate, access and protect information, and its ability to share it throughout the network, allows force elements to operate from common data sets (or 'pictures') of operational information. Consistent throughout the operating space, operational information data sets draw on the same underlying environmental and reference information.

The Joint Operations Picture consists of the Common Operations Picture (COP) and JOP-Web, a tool that can, amongst other things, collate operational reports and returns that reflect the most current information.

IT03.71
MobiKEY Identity Based Access Drive and Defense Identity Management Network

3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●

Mobility. Survivability. Adaptive Dominance.

SPONSOR: Canada
DEVELOPER: Route1, Inc.
CONTACT: Rene McIver, rene.mciver@route1.com

Route1's MobiKEY IBAD and DEFIMNET infrastructure provide military users with the combination of ease-of-use and strong cryptography required for in-theater operations.

MobiKEY IBAD's thumb-sized form factor, coupled with strong multi-factor identification and sophisticated entitlement controls, ensures that warfighters have secure access to the systems and information they need, when and where they need it. The data is never exposed outside of the headquarters' secured network.

When using existing battlefield or naval networks for connectivity, warfighters simply plug their MobiKEY IBAD into a PC for instant access to systems at HQ or at their home command. MobiKEY IBAD can be deployed in both the unclassified and classified domains.

IT03.75
Mobile Tactical Edge Network

3. INTEGRATED OPERATIONS ●
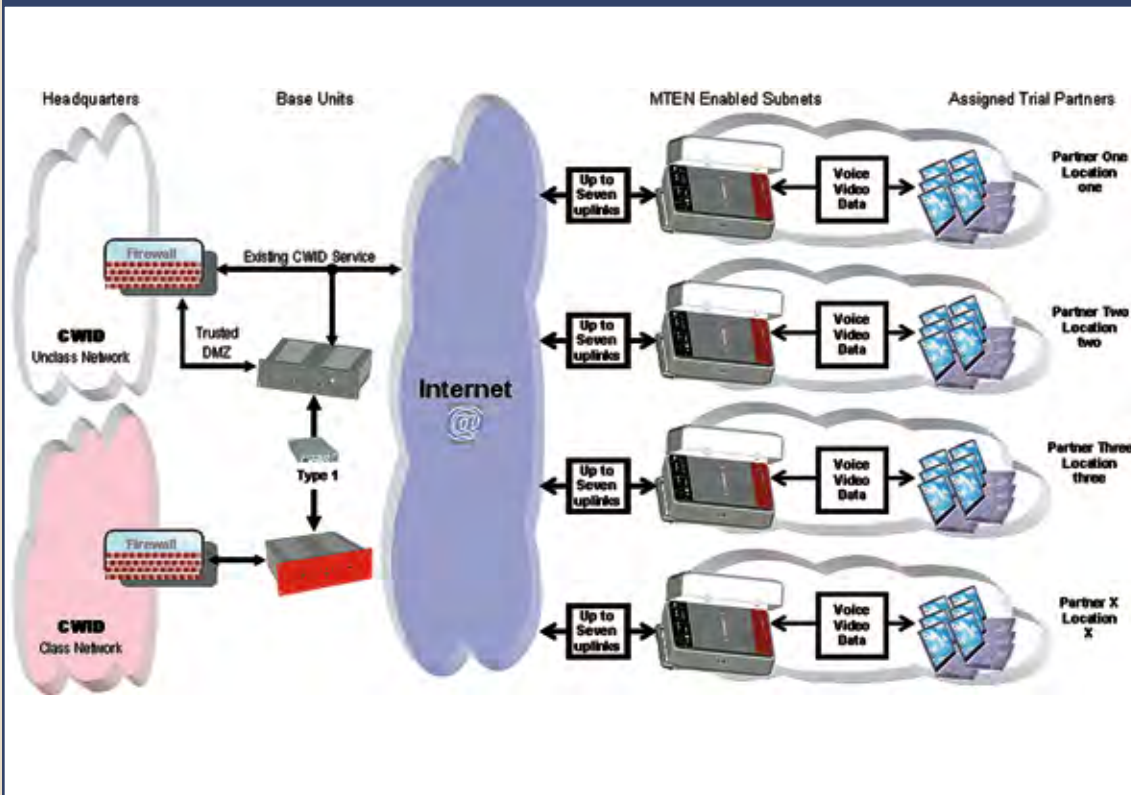
The pTerex MTEN solution enables information sharing at all levels of coalition command. The products are secure, scaleable, and functional at all levels of warfare.

MTEN is non-proprietary. It has been successfully tested for integration and interoperability by U.S. Joint Forces Command (USJFCOM), Naval Special Warfare Command (NAVSPECWARCOM), and Joint Systems Integration Command (JSIC).

MTEN products are non-proprietary, middleware equipment enabling connection to home networks regardless of location. An equipment solution, MTEN provides means to collaborate with existing software and bandwidth capabilities.

MTEN is a lightweight, rugged product suite designed to manage global roaming of mobile networks among and between virtually any current or future network: wired, cellular, 802.11b/g wireless, radio and satellite.

IT03.80
Riverbed Information Optimization System

3. INTEGRATED OPERATIONS ● 4. INTEGRATED LOGISTICS ●
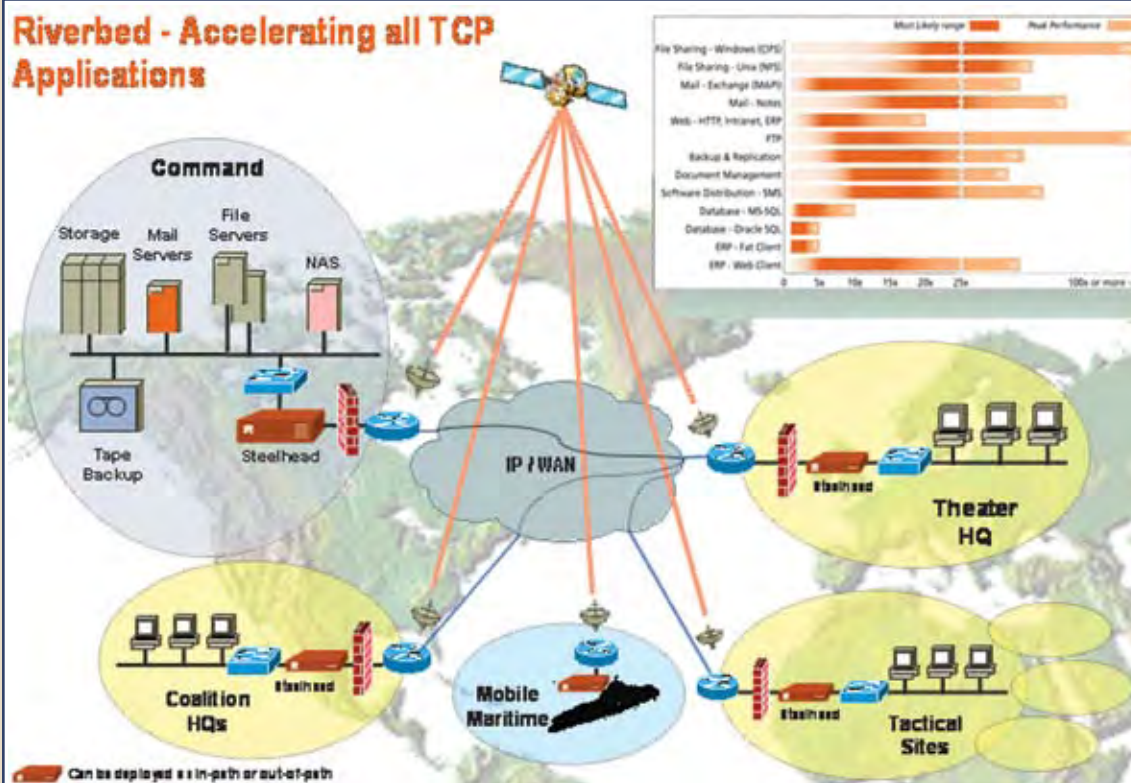
Steelhead appliances (Wide Area Network [WAN] Accelerators), designed and built by Riverbed, eliminate redundant data, optimize performance and reduce latency.

RIOS is high performance and scalable, optimizing all Transmission Control Protocol (TCP) traffic for maximum bandwidth. Additional application-specific optimizations further enhance response times.

RIOS uses a new combination of patented and patent-pending mechanisms to achieve application acceleration. These mechanisms include transaction prediction, TCP proxying and optimization, and hierarchical compression to deliver orders of magnitude increases in application response time and throughput.

IT04.79
Event-based Common Operational Picture

3. INTEGRATED OPERATIONS ● 4. INTEGRATED LOGISTICS ● 5. INTEGRATED PLANNING ●
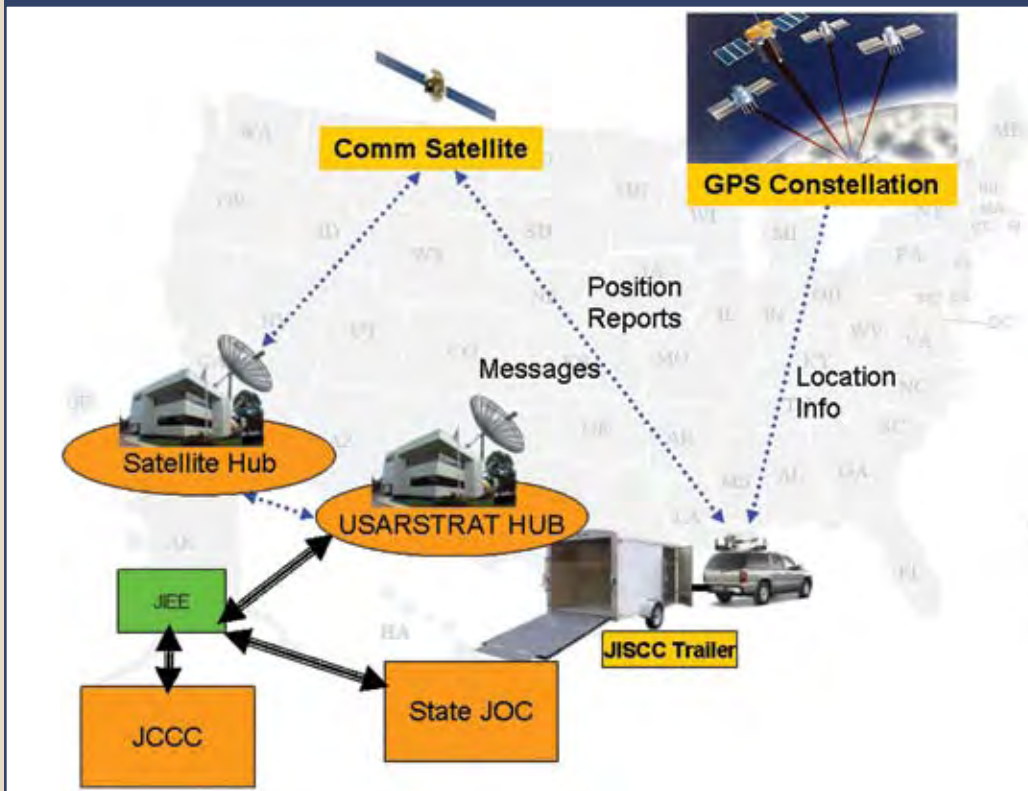
SPONSOR: National Guard Bureau (NGB)
DEVELOPER: Booz Allen Hamilton
CONTACT: Maj. Kory Gacono, kory.gacono@us.army.mil

NGB's Joint CONUS Communications Support Environment (JCCSE) is an umbrella concept including communications and information systems that provide connectivity, collaboration, situational awareness, and C4 coordination among Homeland Defense (HLD) and Defense Support to Civil Authorities (DSCA) mission partners.

ECOP provides Geospatial Information Systems (GIS) visualization of common operational event and asset data, using standards-based tools and symbology. It shares georeferenced event and asset data with all mission partners.

NATIONAL GUARD EVENT-BASED COMMON OPERATIONAL PICTURE WILL:

■ Support improved coordination of distributed operations, enhancing operational agility

■ Enable the NGB Joint C4 Coordination Center (JCCC) to improve coordination and employment of C4 Assets in response to multiple events

IT05.08
Joint Strike Fighter Offboard Mission Support Environment

1. CROSS-DOMAIN DATA SHARING ● 5. INTEGRATED PLANNING ●
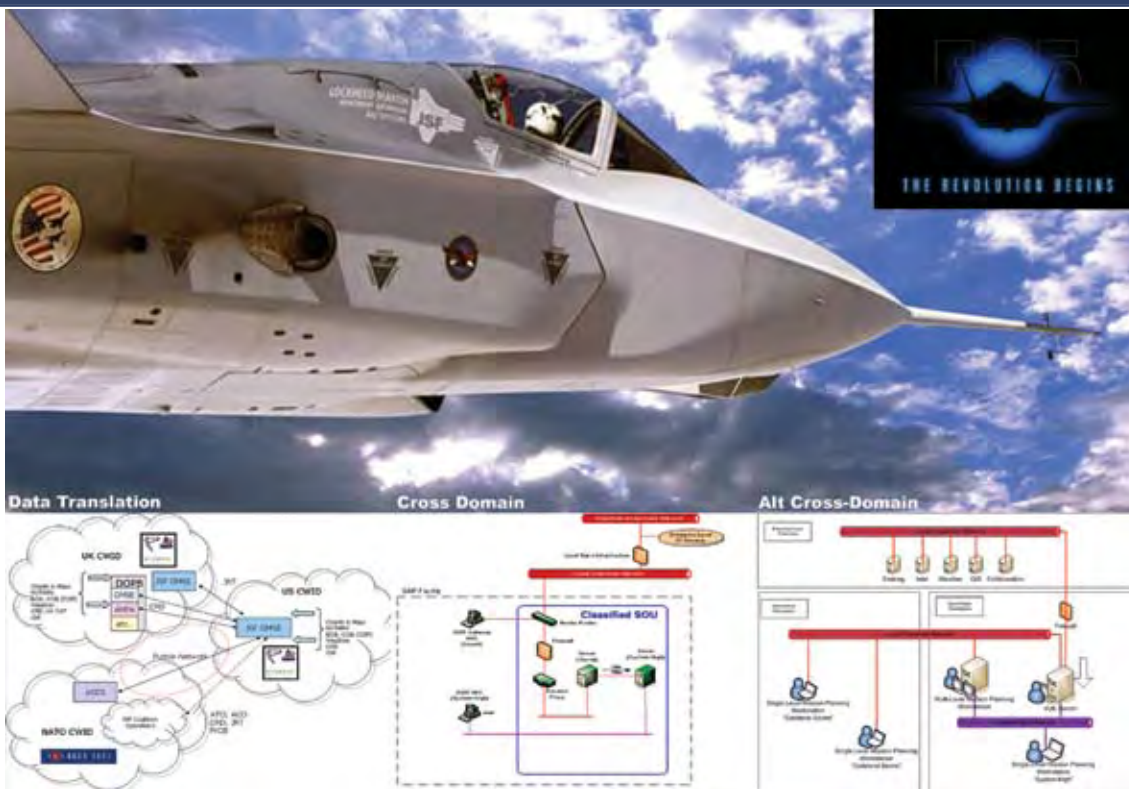
SPONSOR: Joint Strike Fighter (JSF) Program Office
DEVELOPER: Lockheed Martin, Systematic Software Engineering, Naval Mission Planning
CONTACT: David Pearson, david.pearson@jsf.mil

The JSF is a multinational endeavor to develop a common fighter aircraft. OMSE is the JSF's ground based mission planning system. The OMSE is designed to support all aspects of coalition mission preparation and post mission analysis.

The OMSE enables interoperability in the following areas

■ **US/US DATA SHARING:** Mission planning information can be shared with existing mission planning systems.

■ **US/UK/COALITION COLLABORATION:** Strike package coordination information can be shared with other coalition mission planning systems.

■ **US/UK/COALITION DATA EXCHANGE:** Information can be exchanged with NATO's Air Command and Control System as well as with other UK national systems

■ **CROSS SECURITY DOMAIN DATA EXCHANGE:** Essential data can be passed from one security domain level to another.

IT05.12
ID-MAP: Situational Awareness, Visualization and Collaboration

2. INTEGRATED INTELLIGENCE ● 3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●

SPONSOR: USNORTHCOM, US Coast Guard
DEVELOPER: General Dynamics
CONTACT: Mike Barney, mike.barney@gdc4s.com 1.480.441.2205

ID-Map (IC-1) allows multiple users in different locations to collaborate by seeing what others see, automatically sharing each others' information, maps, reports, data, writings, notations, and geospatial images, from most any source — in a way, to virtually see what others are thinking.

ID-Map (IC-1) provides a collaborative environment for Domain Awareness, allowing disparate users to share and analyze information in real-time. ID-MAP is built on CoMotion®, a real-time, decision-making "always on" dynamic, collaborative environment platform. ID-MAP enables decision-makers with actionable intelligence to cross multiple boundaries in real time using collaboration, visualization and analysis.

IT05.59
Mission Planning System

3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●
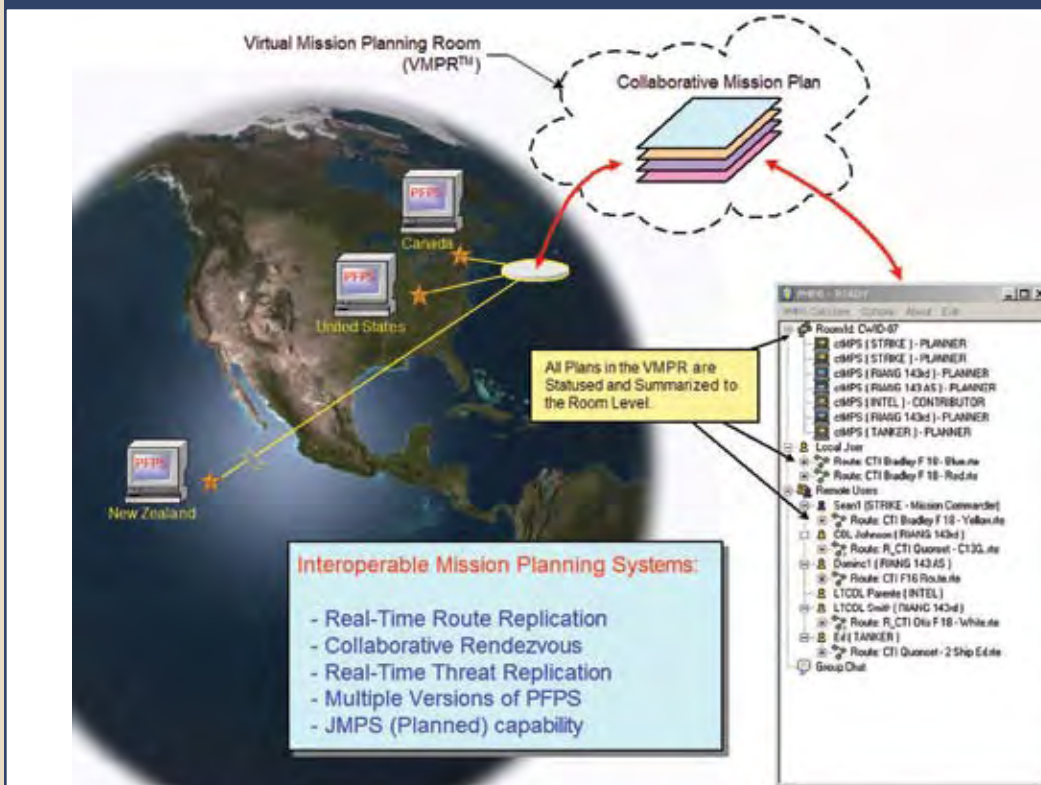
SPONSOR: US Air Force
DEVELOPER: Collaboration Technologies, Inc.
CONTACT: David Buckley, 1.401.234.1145, dbuckley@CollaborationTech.net

MPS is a collaboration-enabled Portable Flight Planning System (PFPS) which allows users to enter a Virtual Mission Planning Room (VMPR). It is simple to use, requiring little additional training beyond operational familiarity with PFPS. MPS provides new capabilities to the mission planner, allowing geographically separated warfighters to collaborate in real time. MPS also provides intelligence to create, input and share threat data symbology, greatly enhancing situational awareness.

Once in a VMPR, each user works on routes and observes routes being created and updated by other users in the virtual room. Whenever anyone makes the slightest change to a route the change will immediately be reflected in the VMPR.
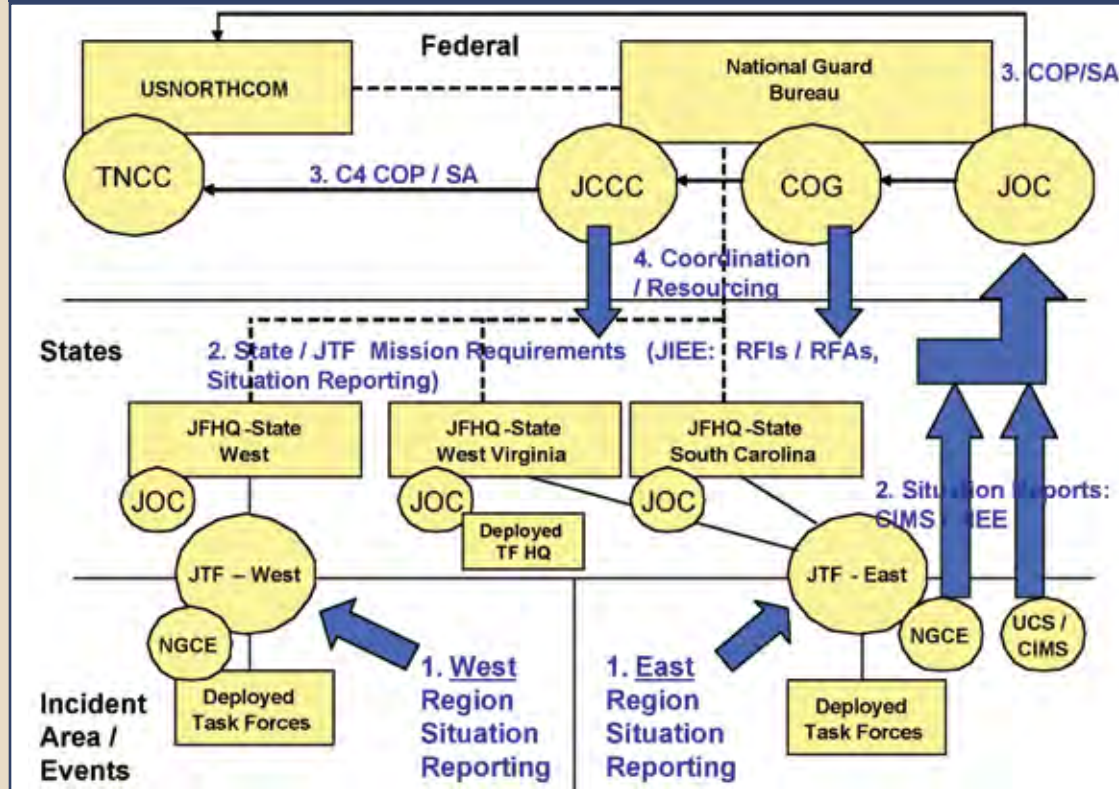
Finally, the MPS Collaborated Rendezvous capability automates steps for creating refueling and mission support rendezvous.

IT05.78
Next Generatrion - Joint Information Exchange Environment

5. INTEGRATED PLANNING ●

NGB's JCCSE, is an umbrella concept to enable the reliable and timely flow of key information to support state and Federal military activities for Homeland Defense (HLD) and Defense Support to Civil Authorities (DSCA). It includes communications systems and programs that provide connectivity, collaboration, situational awareness, and C4 coordination.

JIEE is the JCCSE component supporting information sharing and critical processes, such as tracking and situation reporting.

NG-JIEE WILL:

■ Demonstrate improved situation reporting capabilities that support Essential Elements of Information (EEIs) for support to HLD/DSCA missions

■ Support evaluation of technologies and processes that support collection and dissemination of information across the National Guard and with mission partners focusing on net-centric solutions

IT06.04
Tactical Emergency Asset Management System

6. INTEGRATED COMMUNICATIONS ●

The T.E.A.M. system is a small-footprint, self-deployable system providing net-centric communications for incident commanders and for communications between operational and tactical levels of activity.
CAPABILITIES INCLUDE: Radio bridging between radios used by civil first responders and with land-line, cellular and satellite telephone communications ■ integration between civil first response and military radios ■ satellite broad-band internet connectivity for data, voice-over-internet-protocol (VOIP), and video streaming ■ wireless access ■ satellite television ■ public address system ■ on-board power generation.

The T.E.A.M. system provides the means to synchronize and connect federal, state, local and nongovernmental agencies and organizations with each other and with military organizations to provide an integrated and fused common operational picture to interagency partners.
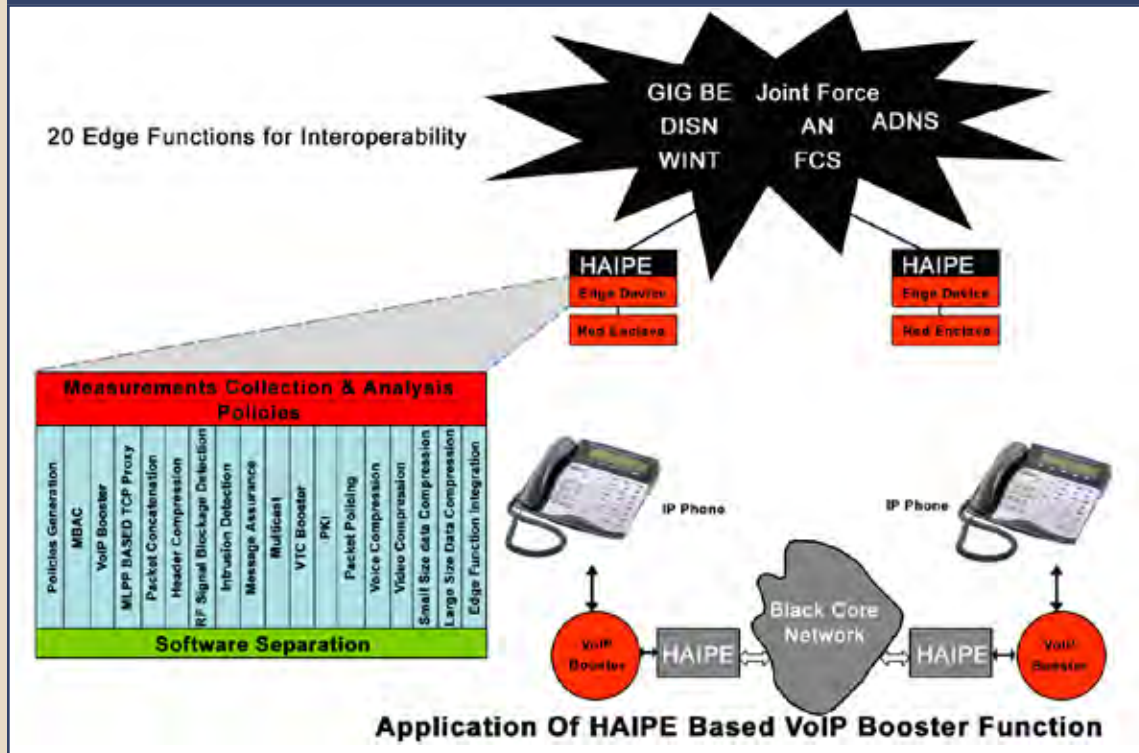
IT06.13
Global Information Grid Quality of Service Edge Solution for Interoperability

6. INTEGRATED COMMUNICATIONS ●

20 Edge Functions for Interoperability

Application Of HAIPE Based VoIP Booster Function

SPONSOR: US Army
DEVELOPER: DSCI
CONTACT: Dr. George Elmasry, gelmasry@dsci-usa.com,

The future military network GIG is envisioned to consist of a seamless black core with many large-scale encrypted networks, each with specific requirements and QoS challenges. While each network meets application-specific QoS expectations, the application might see QoS violations for traffic routed over multiple networks. An interoperability approach is needed to mitigate problems and maximize network resource use.

The top figure shows 20 Edge Functions that are modular based on needs. The lower figure shows the VoIP Booster function application. A Warfighter communicating while traveling through dense foliage or an urban area may experience additional degradations from encryption resulting in higher packet loss. An edge device at both ends of the network mitigates much of this degradation. New standards mandating the use of edge devices on all black core networks ingress/egress points requiring them, will substantially improve the QoS and network performance.

IT06.15
Geolap

6. INTEGRATED COMMUNICATIONS ●

SPONSOR: Canada
DEVELOPER: MCE
CONTACT: Mario Beauchesne, 1.613.992.7727, beauchesne.mc@forces.gc.ca

GEOLAP is a Defense Research and Development Canada (DRDC) Valcartier application that was developed to track production statistics and provide drill down query capability on the production management information for the NTDB (National Topographic Database).

Geolap implements Online Analytical Processing (OLAP) technology, which provides improvements in overall performance. Functionalities include geospatial data search tools and discovery and dissemination capabilities based on ISO 19115 metadata standards.
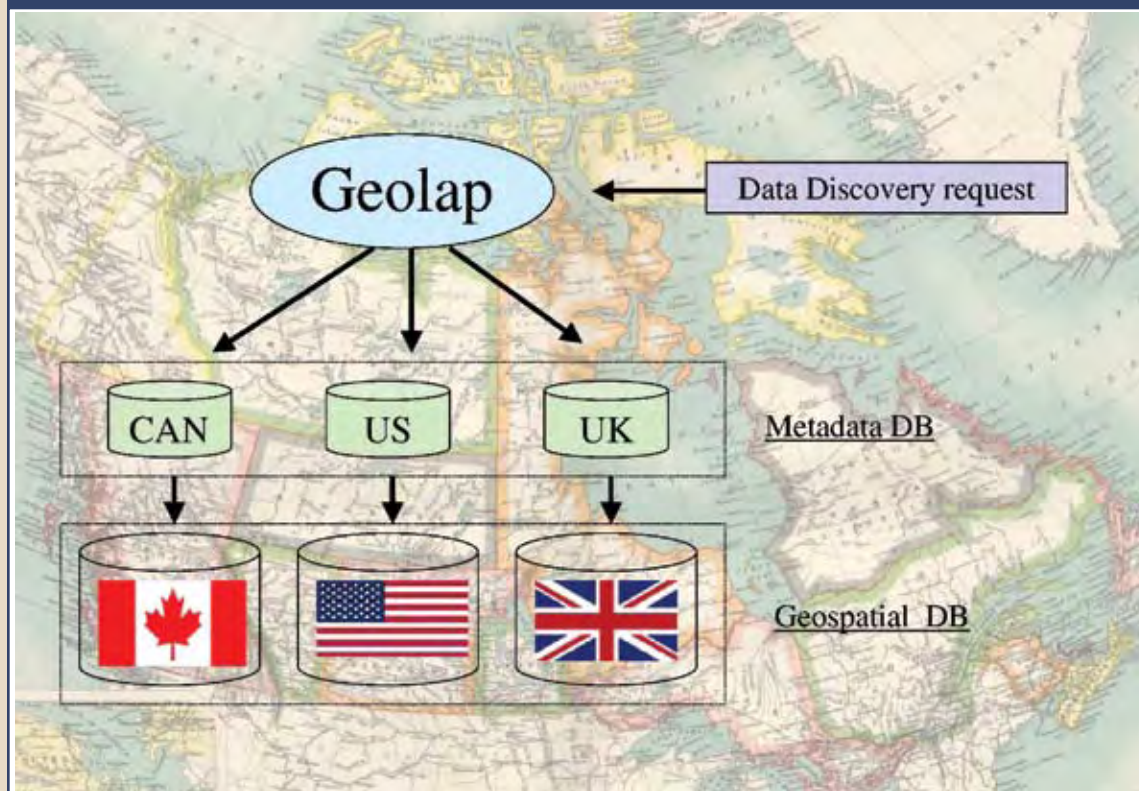
IT06.36
Joint Network Defense and Management System

6. INTEGRATED COMMUNICATIONS ●

JNDMS is an operation-centric network monitoring tool. It helps to answer the "So What?" question when events take place on networks.

JNDMS collects and fuses data from five domains: ■ Information Technology (IT) infrastructure and IT services ■ network incidents and threat events ■ network vulnerabilities and exploits ■ safeguards deployed on the networks ■ military operations.

Data sources include network management sensors, network security sensors, and various databases. JNDMS fuses data and displays information to the user. This information allows the user to understand the state of the networks.
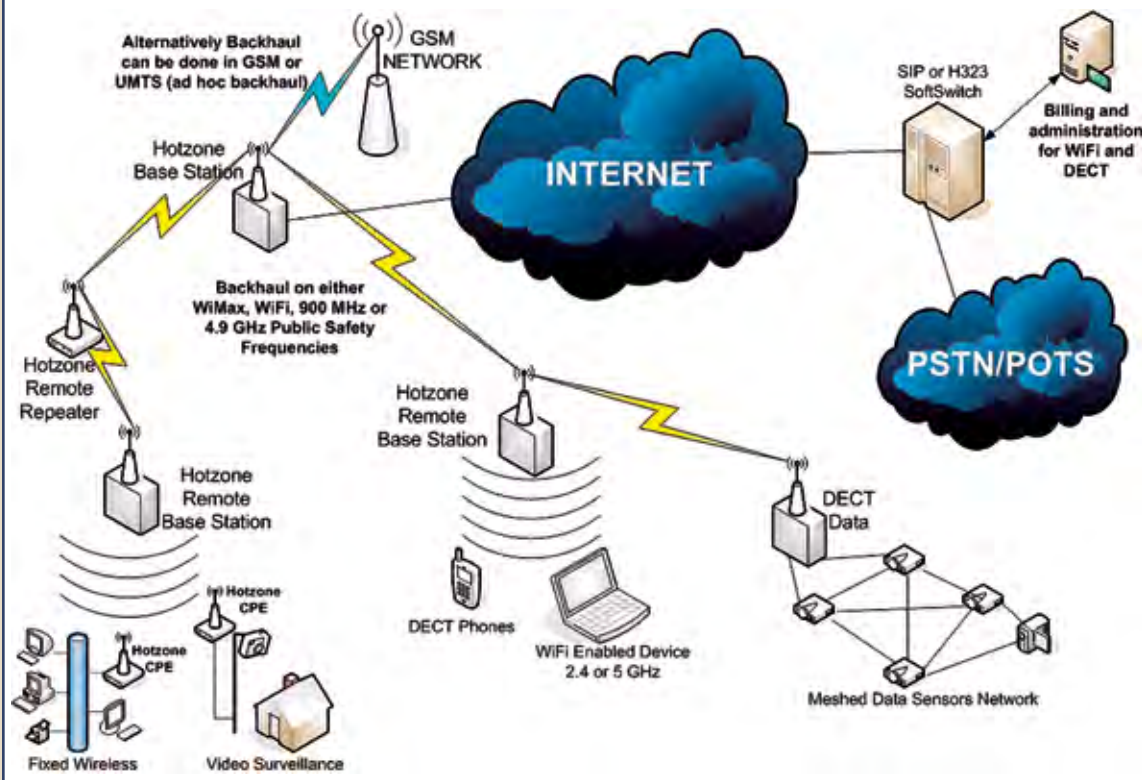
Users can select multiple views, one showing the dependencies of the military operations on the IT infrastructure. JNDMS assesses the severity and impact on military operations of network incidents.

JNDMS also includes a geospatial view of networks.

IT06.42
HotZone 4010/4020

3. INTEGRATED OPERATIONS ● 6. INTEGRATED COMMUNICATIONS ●

Trimax Wireless Inc.'s flexible wireless platform approach provides more than five different applications or combinations. Trimax seamlessly bridges WiMAX, WiFi, 4.9GHz public safety, long-range 900MHz (NLOS) DECT and GSM/UMTS, with ability to rapidly incorporate evolving standards.

APPLICATIONS SUPPORTED BY TRIMAX RADIOS:
Broadband ■ Voice ■ Video ■ Sensor Reading ■ Commercial Sensors ■ Power Meters ■ Gas Meters ■ Water Meters ■ Military Sensors ■ Nuclear/Biological/Chemical Sensors ■ Acoustical/Infrared Sensors ■ Actuators ■ Power Load Control ■ Valve Control

Trimax radios are fully upgradeable. Government organizations will be able to protect their wireless infrastructure investment by deploying equipment that allows future modular upgrades in radio technology without replacing core infrastructure.

IT06.53
Weapons of Mass Destruction Collaborative Advisory and Response System

3. INTEGRATED OPERATIONS ● 5. INTEGRATED PLANNING ●
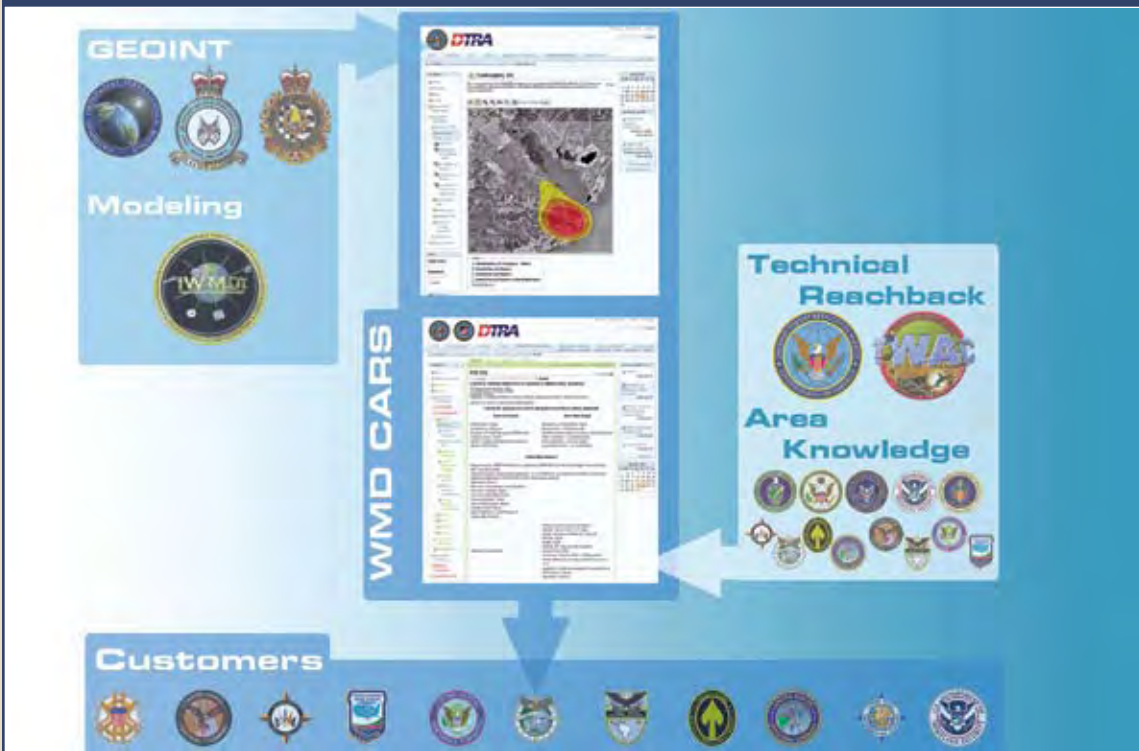
SPONSOR: Defense Threat Reduction Agency (DTRA)
DEVELOPER: DTRA
CONTACT: Maj. Trisha Wilson, trisha.wilson@dtra.mil

WMD CARS enables unprecedented collaboration between DTRA subject matter experts and combatant command/Joint Task Force (JTF) staffs. WMD CARS fuses dissimilar, critical information and distributes it to the strategic decision maker to support consequence management, force protection, and Military Assistance to Civil Authorities (MACA) in the event of hostile chemical, biological radiological, and nuclear (CBRN) events.

This information sharing tool is a multi-use open-framework resource for deliberate and crisis action planning, at strategic and operational levels, that provides a clearer view of the battlefield to the warfighter.

IT06.66
Internet Protocol Interoperability & Collaboration System

6. INTEGRATED COMMUNICATIONS ●
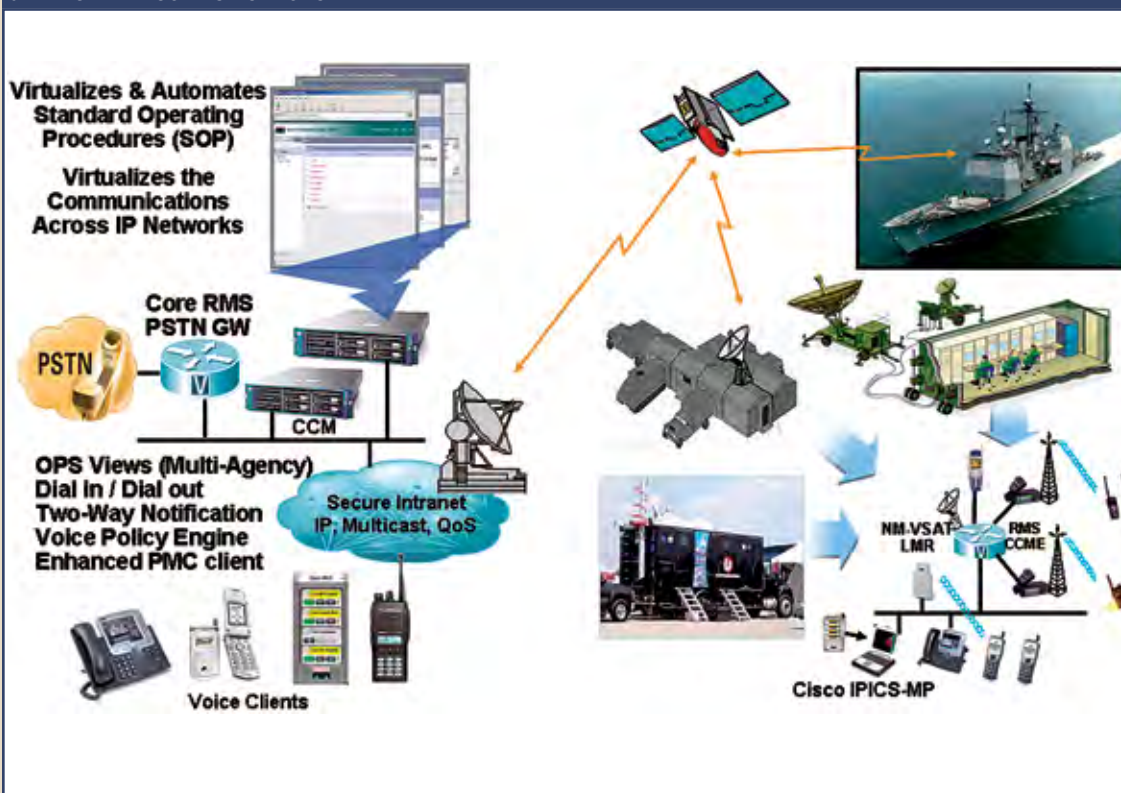
SPONSOR: Canada
DEVELOPER: Cisco Systems, Inc.
CONTACT: Dave West, davwest@cisco.com

CISCO IPICS delivers secure, reliable communications at the point of necessity. The Cisco IPICS solution empowers agencies to collaborate and coordinate across even the most formidable geographies and resource barriers.

Agencies have a communication platform designed specifically for rigorous demands:
■ flexible command and control – centralized or remote
■ improved response time and collaboration with other agencies
■ real-time communications between diverse services

IPICS delivers enhancements to existing applications, equipment and networks:
■ IP network-based solution that provides rugged reliability
■ IP based – leverages IP standards and protocols
■ easily integrated with or built on existing system capabilities and communication networks
■ future-proofed with integrated voice, video and data.

IT06.74
Security Information Management for Enclave Networks

1. CROSS-DOMAIN DATA SHARING ● 6. INTEGRATED COMMUNICATIONS ●
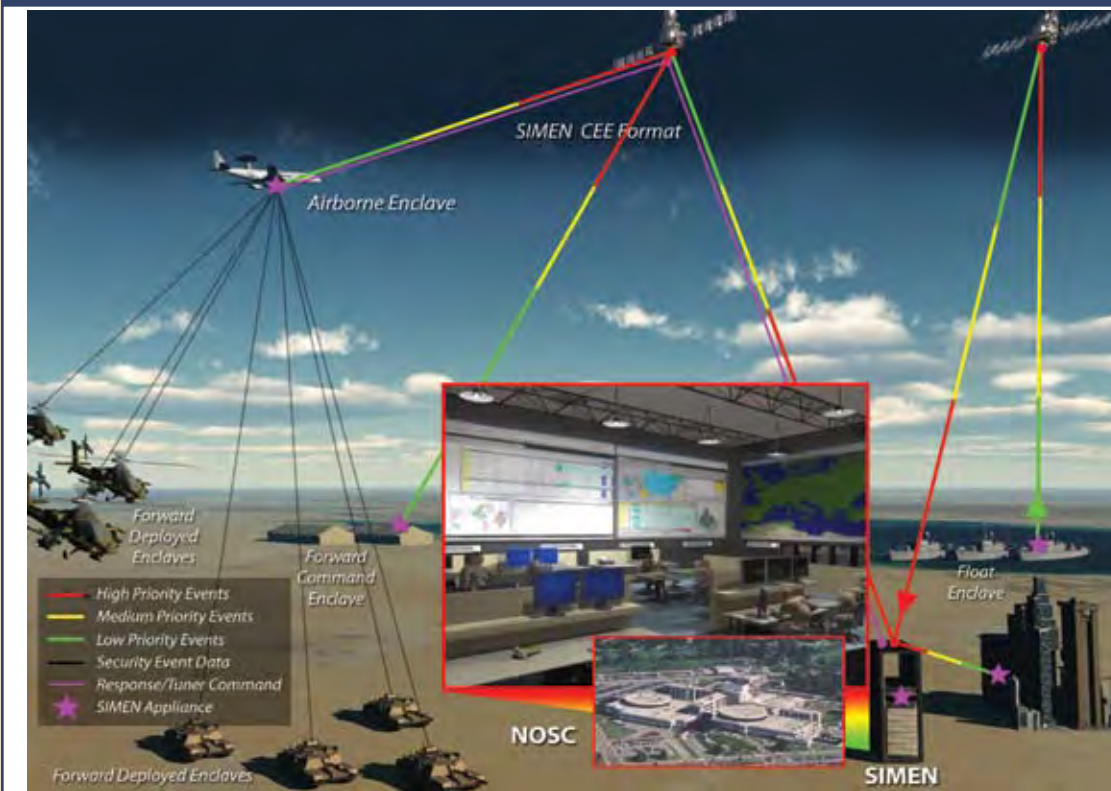
SIMEN Global Information Grid (GIG) Information Assurance (IA) depends upon an enterprise-wide sensor grid that collects and feeds a centralized security monitoring location. Timely, threat-focused collection and security event data processing is challenging with bandwidth constraints, high volumes of data, and rapidly evolving threat environments typical of tactical networks.

The SIMEN research project is prototyping adaptive algorithms and protocols for the distributed collection and predictable, efficient transport of IA events to a central location.

SIMEN uses efficient protocols and adaptive algorithms to dynamically respond to evolving threat environments, respect bandwidth constraints, prioritize events, and minimize fluctuating event volumes. Tactical network (air, land, sea) computer network defense (CND) success depends upon such capabilities.

IT06.89
Enhanced Video Text and Audio Processing

6. INTEGRATED COMMUNICATIONS ●
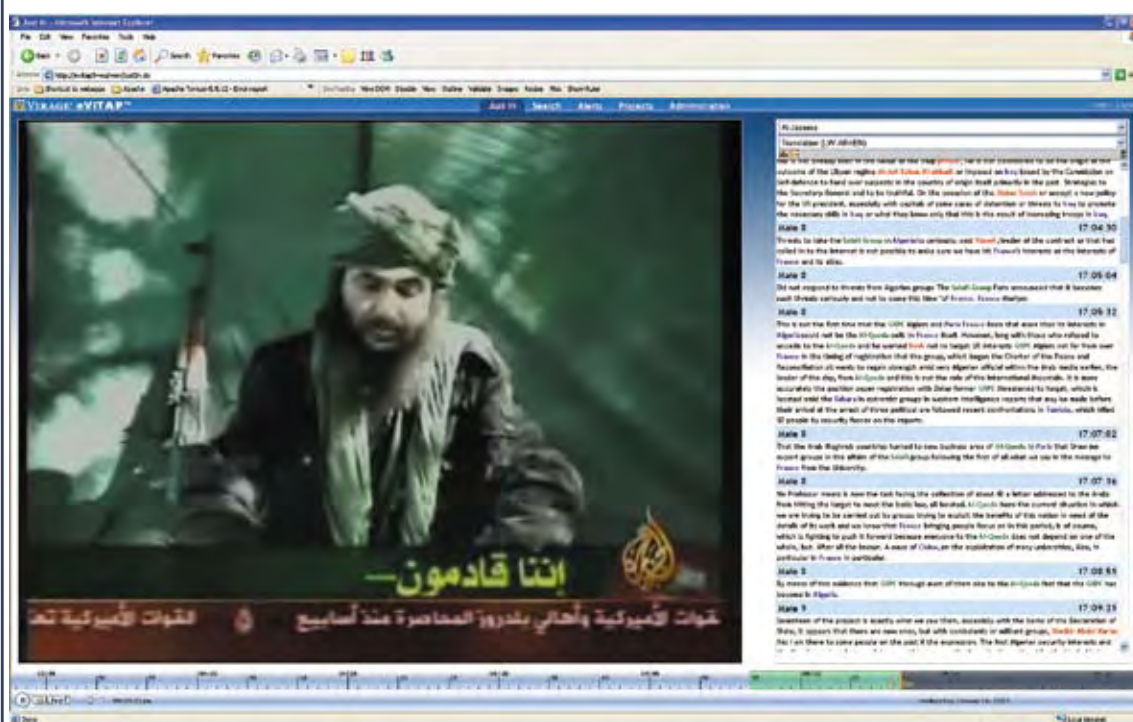
eViTAP provides a fully automated, real-time, multi-lingual, news monitoring capability supporting over 20 languages including Arabic, Chinese, Japanese, Persian, and Russian. It uses a combination of advanced search and automated alerting to monitor multi-lingual news sources in real-time.

Using state of the art technologies, eViTAP transcribes audio into text which is translated into English. Video and images are analyzed for face ID, logo detection, multi-lingual OCR, and closed captioning. Documents are translated into English and processed for automatic detection of people, places and organizations. Results are indexed by an integrated Autonomy IDOL™ search engine.

eViTAP users leverage these powerful technologies via an intuitive, easy to use browser based interface. This interface presents a collaborative environment for quickly and efficiently finding, editing and exporting relevant intelligence.

IT06.90
Optimized Data Environment for NetCentric Operations

6. INTEGRATED COMMUNICATIONS ●

ODEN

Optimized Data Environment for NetCentric Operations

☑ Federal Information Security Management Act (FISMA) compliant

☑ Electromagnetic Interference/Compatbility (EMI/EMC) neutral

☑ Network or Peer-to-peer transmission tools

☑ Data compression factor of 2x - 20x

☑ Improved bandwidth utilization

☑ Optional encryption algorithm (8192 bit SSL or up to 2048 Elliptic Curve) by FIPS 113, 140-2, 180-2 and 197

☑ Improved performance over any media or network

☑ Universal application - network, media, and hardware neutral

☑ Windows, Linux, Mac & Solaris operating systems

solaris

SPONSOR: DISA
DEVELOPER: Total Integrated Medical Management & E-Solutions (TIMMES), Inc.
CONTACT: Stelian-Doru Ticsa, 727.410.1832, doru@timmes.com, Phillip Allison, 727.773.7866, phillip@timmes.com

ODEN PROVIDES:

■ Universal software based advanced communications performance tool

■ 100% lossless file transfer

■ Technology developed, patented and employed with proven results since 2002

■ Improved performance over any media or network

■ Improved bandwidth utilization

■ Assure data integrity

■ Data encryption and compression

■ Universal application: network (RF, copper and fiber, at user, server, router or transmission level), media and hardware (Windows, Linux, Mac, Solaris OS's) neutral

■ FISMA compliant

■ DICOM implementation in OSI applications level 7

■ ACR and NEMA compliant

HISTORY OF CWID

CWID traces more than 16 years of history to establishment of the Secure Tactical Data Network (STDN) series originated by the U.S. Army to demonstrate emerging command, control, communications and computer (C4) capabilities.

STDN 1 and 2 concentrated on Army-only issues while STDN 3 brought the first multi-service participation. The Joint Staff recognized that advances in communications and information technology in the public sector were outpacing Department of Defense (DoD) capabilities.

The Joint Staff assumed sponsorship of the STDN series in 1993 under the C4I for the Warrior concept. The Defense Information Systems Agency (DISA) was directed to be Executive Agent, in concert with a lead Service, to organize network experiments, bringing emerging public sector and other government agency technologies into DoD projects and into war-fighters' sphere of recognition. DISA was also directed to improve joint C4 interoperability.

In 1994, annual STDN efforts evolved into the first Joint Warrior Interoperability Demonstration (JWID). The Air Force was lead service and U.S. Atlantic Command was host combatant command. The idea of moving from a static, one-dimensional picture of the battlefield to a near real-time, multi-dimensional battlespace picture became reality to joint and combined warfighters.

Key efforts in JWID '94 included demonstration of baseline segments of what became the Global Command and Control System (GCCS). Six

weeks after the conclusion of JWID '94, GCCS was operationally deployed to U.S. Atlantic Command supporting military operations in Haiti. Full operational deployment of GCCS to all combatant commanders occurred within 12 months after JWID '94.

In 1997, the Chairman of the Joint Chiefs of Staff mandated interoperability in Joint Vision 2010, envisioning future conflicts as coalition operations. JWID assisted that vision, establishing itself as a coalition interoperability forum through invitations to Combined Communications Electronics Board (CCEB) nations (Australia, Canada, New Zealand and the United Kingdom) and NATO beginning with JWID '94 and continuing to the present. While invited participants used JWID to perform their own technology demonstrations and joint interoperability trials, their main intent was to promote and ensure C4 interoperability with the U.S.

EXPANSION

In 1998, JWID evolved into a two-year process to pursue selection and limited fielding of C4 technologies to warfighting combatant commanders. The Theme (first) Year conducted demonstrations and interoperability trials and selected "Gold Nuggets" for support and continued improvement during the Exploitation (second) Year, with eventual fielding to combatant commands. JWID '98 fielded three Gold Nuggets to warfighters.

U.S. Y2K concerns drove JWID '99-R to focus only upon coalition interoperability trials between the U.S. and CCEB/NATO nations.

To more easily promote trials and other Command, Control, Communications, Computers and Intelligence (C4I) experiments, the Coalition Wide Area Network (CWAN), established annually for JWID, evolved into the standing Combined Federated Battle Laboratories Network (CFBLNet). The network permits C4I experimentation among the U.S. and nations of CCEB/NATO year-round, using systems jointly owned and managed by CFBL membership.

JWID '00-'01 restored the two-year cycle, with 23 U.S. demonstrations and 145 combined/coalition demonstrations worldwide. Two Gold Nuggets were fielded in 2001. In addition, a Distributed Collaborative Tool Set (DCTS, now Defense Collaboration Tool Suite) was refined and subsequently selected for worldwide fielding to the Unified Commands. DISA fielded the capability, within 72 hours, in support of the Office of the Secretary of Defense (OSD) requirements following terrorist attacks of September 11th, to multiple DoD networks.

COALITION INTEROPERABILITY

JWID 2002 featured transition from a limited fielding of technology to full focus on coalition interoperability, led by U.S. Pacific Command (USPACOM), the host combatant command. The demonstration included Pacific Rim nations in a Pacific Theater Initiative (PTI), with Japan, South Korea, Singapore, and Thailand participating while Malaysia and the Philippines observed operations. Coalition partners were integrated on the Multinational Task Force (MTF) and component staffs to maximize opportuni-

ties. The JWID CWAN continued use of CF-BLNet architecture and services established in past demonstrations. U.S. Joint Forces Command (USJFCOM) fielded a JWID demonstrated language translation device.

JWID 2003 took coalition interoperability to new heights. USPACOM guided the CTF and, for the first time, Japan, South Korea, Thailand and Singapore provided staffing to expand information exchange over dual domains. One key focus for 2003 included management of information exchange between the traditional 6-eyes network to a larger, more robust 10-eyes network. The larger network was vital to JWID's success because Pacific Rim nations needed effective information to serve in MTF staff positions. JWID 2003 addressed multi-level security technical solutions and refinement of coalition policies and procedures to overcome issues surrounding information exchange.

DISA assumed duties as the lead agency, providing broad-base management support of JWID activities. Four Coalition Interoperability Trials (CITs) with especially noteworthy performance were submitted to USJFCOM J861, for consideration for limited fielding.

HOMELAND SECURITY

JWID 2004 featured U.S. Northern Command (USNORTHCOM) as the Host Combatant Command. USNORTHCOM brought a Homeland Security/Homeland Defense (HS/HD) focus to the demonstration. This approach broke new ground beyond the traditional JWID coalition interoperability area, adding government interagency information sharing. USNORTHCOM, in a departure from previous JWIDs, invited agencies within the Department of Homeland Security, including first-time participation for the Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation (FBI), the U.S. Coast Guard, and the National Guard Bureau. Limited coalition participation between these organizations occurred as Canada's Office of Critical Infrastructure Protection joined in the interoperability trials. This activity offers significant potential for more extensive cooperation between other coalition homeland security organizations and their U.S. counterparts. USJFCOM filled an ancillary role, assisting with select fielding of technologies to combatant commanders. JWID 2004 involved 25 countries, military services, and government agencies participating in a scripted scenario over a global network.

USNORTHCOM was host Combatant Command in 2005 as the demonstration moved forward with a name change. Now the Coalition Warrior Interoperability Demonstration (CWID), the shift from "Joint" to "Coalition" describes the larger community of participants, including national and international government agencies. A new name was not the only change for CWID in 2005.

USJFCOM formally assumed oversight for planning and execution of CWID 2005 from the Joint Staff in July 2004. This involvement brings USJFCOM advocacy for U.S. combatant command interoperability shortfall resolution to the forefront. USJFCOM's objectives include (1) to ensure CWID demonstrates relevant technologies that address combatant commander's capability gaps, (2) to investigate military, coalition

and interoperability solutions and (3) to identify technologies suitable for prototype initiatives.

CWID 2005 featured revitalization of the planning and collaboration web site, including readily accessible general information. Online trial submission abbreviated initial proposal processes for interested technology representatives. Additionally, CWID established a Concept of Operations (CONOPs) for all recurring aspects of planning and execution.

The CWID 2005 Execution results were noteworthy in that most ITs successfully achieved their stated objectives. More than 400 operators from the military and supporting agencies, at multiple U.S. and coalition sites, executed the scenario events to evaluate and report on trial performance.

Fifteen trials were considered "success stories," moving forward for continued development. Seven ITs were selected for Service, Agency, or limited Combatant Commander fielding (including fielding in support of Hurricane Katrina). Two ITs achieved milestones and continue spiral development as Programs of Record. One was selected for funding via a Congressional Plus-up for further research and development, and one was submitted as a Limited Acquisition Authority candidate. Four others were identified for agency fielding in some capacity.

U.S. European Command (USEUCOM) is the host combatant command for 2006 through 2008. USNORTHCOM continues as the lead for HS/HD CWID operations.

TRIAL HIIGHLIGHTS 2006

PIPELINE TECHNOLOGIES AND OUTCOMES

■ Four trials were Programs of Record (POR) conducting spiral development

1. Integrated Information Management Systems (IIMS): was a U.S. Air Force/AFRL R&D effort that continues spiral development in 2007; involved in transition agreements with JWARN and JEB PORs.

2. Coalition & Civil Agency Capable Wireless Information Transfer System (C3WITS): communications suite embarked on two U.S. Navy aircraft carriers; slated for further purchase

3. Intelligent Road/Rail Information Server (IIRIS): U.S. Army sponsored technology and POR; government owned; expanded utility to include U.S. Transportation Command (US-TRANSCOM)

4. HLS/D Collaborative Information Exchange Environment (CIEE): NGB sponsored POR; continuing spiral development in 2007 as Joint Collaborative Information Exchange Environment.

■ One trial a System of Record conducting spiral development

1. Wide Area Interoperability System (WAIS) & ACU 1000: sponsored by USNORTHCOM; successfully demonstrated stated objectives; picked-up on the GSA schedule; Department of Homeland Security (DHS) and Federal Emergency Management Agency (FEMA)

purchased technology as core of Mobile Disaster Response Vehicles

■ Two demonstrations picked up for purchase

1. Incident Commander's Radio Interface (ICRI): technology participated as a trial in 2005; demonstrated at Dahlgren during 2006; real-world success in Katrina crisis response; purchased by U.S. Marine Corps and DHS for disaster response

2. "Buster:" UAS late entry in 2006; demonstrated well at Dahlgren; units purchased by U.S. Marine Corps and United Kingdom for immediate training and deployment.

TRIAL HIGHLIGHTS 2005

PIPELINE TECHNOLOGIES AND OUTCOMES

■ One trial Limited Acquisition Authority (LAA) candidate:

1. Multi-level-secure Information Infrastructure (MI2): considered by USNORTHCOM for submission as Urgent Need Statement (UNS), LAA request; U.S. Joint Forces Command (USJFCOM)/Joint Systems Integration Command (JSIC) military utility assessment; USNORTHCOM chose not to submit UNS; LAA did not go forward at USJFCOM

■ Two trials targeted for further testing

1. Advanced Geospatial Imagery Library Enterprise (AGILE): further development by National Geospatial-Intelligence Agency (NGA) into a near-term operational capability; currently being assessed by JSIC as part of the JBSA initiative; included as baseline technology for transmitting imagery

2. Posted Applications Over Return Channel Satellite: Global Broadcast System (GBS) continues spiral development in JUICE 06; DoD POR that supports service interests in field today.

■ One trial funding identified, Congressional Plus-up

1. Masking Shunt: funded for continued ONR evaluation; received second year of congressional funding for continued testing at JSIC

■ Three trials are Programs of Record

1. Commercial Joint Mapping Tool Kit (CJMTK): CWID venue used successfully for spiral development

2. Joint Warning and Reporting Network (JWARN): CWID used successfully for spiral development; has successfully completed a JSIC planned assessment as part of DJC2 GCCS 4.0 Interoperability Demo

3. Joint Tactical COP Workstation (JTCW): CWID venue used successfully for spiral development

■ Two trials used in U.S. hurricane relief efforts

1. Incident Commanders' Radio Interface (ICRI): USNORTHCOM and numerous civil law enforcement activities purchased technology in support of HS/HD; U.S. Marine Corps purchased and installed ICRI in Rapid Response Vehicles to interface with civil authorities in the event of a crisis response; ICRI used effectively to support Katrina relief efforts; U.S. Marine Corps and DHS fielded units following 2006 demonstration

2. ARINC Wireless Interoperability Solution (AWINS: used effectively to support hurricane Katrina relief effort; gone on to commercial success outside of DoD

■ Two trials proposed for limited combatant commander fielding

1. Multi-Level Chat (MLC): continues JSIC evaluation under Automated Information Security (AIS) umbrella; proposed fielding in response to Urgent Need Statement (UNS), IRAQ; approved by DSAWG for use in Trident Warrior and retention by Navy thereafter for operational use

2. One Way File Transfer (OWFT): continues JSIC evaluation under AIS umbrella for proposed fielding in response to U.S. Central Command (USCENTCOM) UNS in IRAQ proposed for CENTCOM; latest version in NSA Certification, Test & Evaluation; continues

■ Two trials had limited U.S. Marine Corps/Service fielding

1. Tactical Medical Coordinating System (TacMedCS): deployed to IRAQ to support operations

2. Marine Air-Ground Task Force Continuity of Operations System (MAGTFCS: deployed to IRAQ to support ongoing operations

■ One trial for agency fielding

1. Pliable Display Technology: NGA prototype, developed as a near-term operational capability, now fielded

NOTES

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____